Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Бурумбаева А.Р. Преступления в сфере информационных технологий // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2016. – № 10 (ноябрь). – АРТ 81-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ЮРИДИЧЕСКИЕ НАУКИ

УДК 343

Бурумбаева Асель Рифхатовна,
студентка магистратуры
Институт информационных технологий и коммуникаций
ФГБОУ ВПО «Астраханский государственный технический университет»
г. Астрахань, Российская Федерация
e-mail: aselya.95-95@mail.ru

ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: В статье рассмотрены основные виды киберпреступлений и способы защиты от них.

Ключевые слова: киберпреступлениие, интернет-аукцион, мошенничество, уголовная ответственность.

Burumbaeva Asel Rifkhatovna
master student
Institute of Information Technology and Communications
FGBOU VPO "Astrakhan State Technical University"
Astrakhan, Russian Federation
e-mail: aselya.95-95@mail.ru

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

CRIME IN INFORMATION TECHNOLOGY

Abstract: The article describes the main types of cybercrime and how to protect against them.

Keywords: cybercrime, Internet auction fraud, criminal liability.

Преступления в сфере информационных технологий (киберпреступление) - уголовно наказуемые действия, подразумевающие несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных. При этом компьютер выступает в качестве предмета преступления, а информационная безопасность – объекта. К событиям, связанным с преступлением можно отнести ситуации, при которых компьютер – орудие для свершения преступлений, с целью нарушения авторских прав, общественной безопасности, прав собственности, нравственности.

Способы защиты от киберпреступности базируются на следующих основных принципах:

- получение четкой информации о личности или организации, с которой вступают в деловые отношения (полные паспортные данные, почтовый адрес физического лица, юридический адрес и банковские реквизиты организации, телефон и адрес электронной почты, расположенной не на бесплатном сервере, а у платного провайдера).
- использование электронных сертификатов и безопасных протоколов передачи данных;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- непредоставление продавцам реквизитов пластиковых карт и паспортных данных (для этого существуют биллинги и авторизационные сервера процессинговых центров);
- использование кредитных карт (в этом случае возврат денег или чарджбек осуществляется значительно быстрее и проще, нежели при использовании других средств платежа).

Основные рекомендации, разработанные специалистами Центра анализа интернет-мошенничества – Internet Fraud Complaint Center на основе анализа совершённых преступлений:

- обязанности покупателя интернет-аукциона возникают только после того, как продавец выполнит свои обязательства;
- нежелательно покупать товары на сайтах, базирующихся в других странах;
- нужно уточнять у продавца – кто будет доставлять купленный товар, как, когда и каким образом можно будет вернуть непонравившийся или бракованный товар, кто оплачивает его пересылку;
- если продавцы товаров на интернет-аукционе предлагают договориться напрямую, это может сэкономить деньги, а может и помочь в совершении мошенничества, поскольку интернет-аукционы могут обеспечивать страхование заключаемых на них сделок.

Способы защиты от мошенничества при использовании пластиковых карт:

- наиболее простым способом снижения вероятности потерь от мошенничества является ограничение функциональности пластиковой карты совместно с подключением к услуге мониторинга активности (например, в форме SMS-сообщений обо всех операциях с карт-счетом). Для ограничения функциональности пластиковой карты используются:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

лимит на максимальную сумму покупки, максимальное количество операций, максимальную сумму операций по одной карте, ограничение региона использования карты, блокировка карты на то время, пока она не используется и т.д.;

- желательно использовать пластиковые карты, имеющие страховой полис;
- никогда никому (включая работников банка) не сообщать ПИН-код карты и не вводить его на виду у посторонних;
- хранить карту в надёжном месте, недоступном для мошенников;
- в случае потери карты оперативно связаться с банком и заблокировать её использование. В этом случае многое зависит от содержания договора на открытие карт-счёта. Например, клиент по договору может нести ответственность за все операции со своей пластиковой картой в течении N-го числа дней с момента подачи письменного заявления об утере или клиент должен самостоятельно оплачивать блокировку карты (желательно избегать использования данных пунктов в договоре);
- избегать оплаты с помощью голосовой авторизации, снятия слипов импринтером в тех торговых заведениях, надёжность которых вызывает сомнения: есть риск, что с карты снимут большую сумму, чем требуется, либо скопируют данные с магнитной полосы специальным прибором;
- в случае отказа в авторизации нужно проконтролировать факт уничтожения слипа сотрудником торгового предприятия;
- совершая покупки в Интернете, любую информацию, касающуюся карт, следует передавать только по защищённым протоколам, например, протоколу SSL 3.0, с длиной ключа шифрования не менее 128 бит;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- необходимо своевременно проверять выписку по карте (стейтмент).

Существуют строго оговоренные сроки, в течение которых можно выставить претензию обслуживающему банку (чарджбек). Своевременное выставление претензий снимает с клиента ответственность за дальнейший ход событий.

Кроме того, жертвы киберпреступности могут обратиться в следующие структуры:

1. Международная веб-полиция – International Web Police (www.web-police.org/forms/wp_crimereport.html). Сайт специализируется на международных преступлениях. В случае мошенничества содержание заполненной жертвой формы будет передано в соответствующие правоохранительные органы страны, граждане которой участвуют в афёре. Web Police тесно сотрудничает со спецподразделениями, которые занимаются интернет-преступлениями.

2. Центр анализа интернет-мошенничества – Internet Fraud Complaint Center (www.ifccfbi.gov/cf1.asp). Сайт поддерживается американским Федеральным бюро расследований и, соответственно, чаще всего занимается преступлениями, которые произошли в США или как-то задели интересы американских граждан. Между тем сотрудничество ФБР с правоохранительными органами других стран позволяет надеяться на то, что проблема расследования преступлений в других странах все-таки будет решена.

3. Международная группа по борьбе с киберпреступностью Евросоюза – European Network and Information Security Agency (ENISA) имеет право регулирования деятельности стран-участниц ЕС (http://www.enisa.eu.int/).

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

4. Федеральная служба безопасности Российской Федерации (www.fsb.ru/contact/contact.html). В случае если мошенник или жертва – гражданин России можно обратиться в соответствующие спецслужбы. Российские правоохранительные организации активно занимаются киберпреступлениями. Как и в предыдущих случаях, подобные службы ценят как можно более подробную информацию о преступнике.

5. Рабочая группа Anti-Phishing Working Group (www.antiphishing.org/) занимается борьбой с использованием фишинга.

6. Официальный сайт Центра исследования проблем компьютерной преступности (http://www.crime-research.org/).

Уголовная ответственность в РФ

По УК РФ преступлениями в сфере компьютерной информации являются:

- Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Сюда относятся взлом веб-ресурса, подмена главной страницы сайта (дефейс), подбор паролей, взлом БД, проникновение в сеть компании и т.п.

Для привлечения лица к уголовной ответственности недостаточно лишь одного факта совершения им неправомерного доступа к охраняемой законом компьютерной информации. Уголовно наказуемы лишь те деяния, которые повлекли материальные последствия в виде: уничтожения и/или блокирования, модификации, копирования компьютерной информации. Случаи типа подмены главной страницы сайта или простое вторжение обычно не преследуются из-за высоких издержек. Однако, если существенно

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

пострадала ваша инфраструктура или корпоративная репутация, возможно, имеет смысл выдвинуть уголовное обвинение против атакующего.

- **Создание, использование и распространение вредоносных компьютерных программ** (ст. 273 УК РФ). Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Под данную категорию подпадают троянские кони, бекдоры, шеллкоды, руткиты, ботнеты, черви, вирусы, эксплоиты и т.п; DDOS-атаки.

- **Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей** (ст. 274 УК РФ). Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Обращает на себя внимание тот факт, что за преступления, предусмотренные данной статьей, не был осужден ни один человек. Известны лишь единичные случаи, когда за нарушение данной статьи кого-либо штрафовали. Так, например, системный администратор одного из московских банков допустил крах БД. В результате он выплатил штраф в размере 50 тыс. рублей.

Зачастую совершение преступлений в сфере компьютерной информации сопряжено с совершением иных уголовно наказуемых деяний, в

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

частности, таких как нарушение тайны переписки (ст.138), нарушение авторских и смежных прав (ст. 146 УК РФ), кража (ст. 158), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165), мошенничество (ст. 159) и пр.

- Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138. Глава 19. Преступления против конституционных прав и свобод человека и гражданина). Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

- Мошенничество в сфере компьютерной информации (ст. 159.6. Глава 21. Преступления против собственности**)**. Хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Как правило, Управление К занимается мошенничеством, если украли свыше 3 миллионов рублей.

На сегодняшний день до 80% обращений, поступающих через интернет-сайт МВД РФ, посвящены мошенничеству при покупке товаров посредством социальных сетей и в интернет-магазинах.

- Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст.183. Глава 22. Преступления в сфере экономической деятельности). Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Специалисты Управления «К» отмечают в 2014 году стремительное развитие вредоносных программ для банкоматов. Такие вредоносные программы могут иметь довольно широкий функционал, от получения данных банковских карт, включая PIN-коды, до снятия всех имеющихся в банкомате наличных денег и несанкционированного проникновения во внутреннюю сеть банка.

В России борьбой с преступлениями в сфере информационных технологий занимается Управление «К» МВД РФ.

Список использованной литературы:

1. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники. Ижевск, 2014.
2. Лысов Н.Н., Салтевский М.В. Новый подход в технологии собирания и исследования информационных следов // Эксперт-криминалист. 2012.
3. Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий. Краснодар, 2014.
4. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера. Красноярск, 2012.

Дата поступления в редакцию: 20.11.2016 г.
Опубликовано: 22.11.2016 г.