ТЕМА 3: ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Общие положения

В данной теме мы рассмотрим некоторые аспекты законодательства Республики Беларусь, регулирующего правоотношения в сфере ответственности за совершение противоправных деяний, связанных с ИТ-технологиями.

Согласно Гражданскому кодексу Республики Беларусь (далее ГК) можно выделить следующие виды объектов гражданских прав:

- вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права;
- работы и услуги;
- охраняемая информация;
- исключительные права на результаты интеллектуальной деятельности (интеллектуальная собственность);
- нематериальные блага.

В случаях и порядке, установленных ГК и иным законодательством, признается исключительное право (интеллектуальная собственность) гражданина или юридического лица на охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ и услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.).

Использование результатов интеллектуальной собственности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя.

В прошлой теме мы уже рассматривали понятие коммерческой тайна. В ГК дается следующее понятие служебной и коммерческой тайны:

Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Условия правовой охраны нераскрытой информации

Согласно статьи 1010 ГК лицо, правомерно обладающее технической, организационной или коммерческой информацией, в том числе секретами производства (ноу-хау), не известной третьим лицам (нераскрытая информация), имеет право на защиту этой информации от незаконного использования, если соблюдены условия, установленные пунктом 1 статьи 140 настоящего Кодекса.

Право на защиту нераскрытой информации от незаконного использования возникает независимо от выполнения в отношении этой информации каких-либо формальностей (ее регистрации, получения свидетельств и т.п.).

Лицо, без законных оснований получившее или распространившее нераскрытую информацию либо использующее ее, обязано возместить тому, кто правомерно обладает этой информацией, убытки, причиненные ее незаконным использованием.

Если лицо, незаконно использующее нераскрытую информацию, получило ее от лица, которое не имело права ее распространять, о чем приобретатель информации не знал и не должен был знать (добросовестный приобретатель), правомерный обладатель нераскрытой информации вправе потребовать от него возмещения убытков, причиненных использованием нераскрытой информации после того, как добросовестный приобретатель узнал, что ее использование незаконно.

Лицо, правомерно обладающее нераскрытой информацией, вправе потребовать от того, кто ее незаконно использует, немедленного прекращения ее использования. Однако суд с учетом средств, израсходованных добросовестным приобретателем нераскрытой информации на ее использование, может разрешить ее дальнейшее использование на условиях возмездной исключительной лицензии.

Лицо, самостоятельно и правомерно получившее сведения, составляющие содержание нераскрытой информации, вправе использовать эти сведения независимо от прав обладателя соответствующей нераскрытой информации и не отвечает перед ним за такое использование.

Ответственность за разглашение коммерческой тайны также предусмотрена Уголовным кодексом Республики Беларусь (далее УК РБ). Согласно статье 255 умышленное разглашение коммерческой или банковской тайны без согласия ее владельца при отсутствии признаков преступления, предусмотренного статьей 254 УК РБ, лицом, которому такая коммерческая или банковская тайна известна в связи с его профессиональной или служебной деятельностью, повлекшее причинение ущерба в крупном размере, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

То же действие, совершенное из корыстной или иной личной заинтересованности, - наказывается ограничением свободы на срок до четырех лет или лишением свободы на срок до пяти лет.

3.2. Преступления в сфере высоких технологий

Первое высокотехнологичное преступление на территории нашей республики было зарегистрировано 20 ноября 1998 года. Внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием «BackOrifice», злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет из числа клиентов крупнейшего в Беларуси столичного сервис-провайдера.

В 2001 году руководство МВД республики проанализировало криминогенную ситуацию, складывающуюся в сфере компьютерной информации и телекоммуникаций в нашей стране, а также странах дальнего и ближнего зарубежья, принимая во внимание правонарушения, зарегистрированные в 1998–2000 годах, вступление в действие нового Уголовного кодекса, предусматривающего ответственность за преступления против информационной безопасности, а также высокую степень вероятности дальнейшего распространения киберпреступности на территории нашей республики, было принято решение о создании подразделения, специализирующегося на профилактике и раскрытии злодеяний данной категории.

На данный момент раскрытием высокотехнологичных преступлений занимается Управление по раскрытию преступлений в сфере высоких технологий МВД РБ.

На протяжении последних 8 лет количество официально зарегистрированных преступлений в сфере высоких технологий постоянно растет (правда стоит отметить, что темпы прироста постепенно снижаются).

- в 2007 году – зарегистрировано 996 преступлений;
- в 2008 – 1614 (+618);
- в 2009 – 2154 (+540);
- в 2010 – 2514 (+360).

Далее приведены статьи УК РБ, предусматривающие ответственность за высокотехнологичные преступления.

Статья 212. Хищение путем использования компьютерной техники
1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации – наказывается штрафом, или лишением права занимать определенные

должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.
2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, – наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.
3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные в крупном размере, – наказываются лишением свободы на срок от трех до десяти лет с конфискацией имущества или без конфискации и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.
4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, – наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Глава 31.Преступления против информационной безопасности

Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом или арестом на срок до шести месяцев.
2. То же действие, совершенное из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.
3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Модификация компьютерной информации

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) - наказываются штрафом, или лишением

права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.
2. Модификация компьютерной информации, сопряженная с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, - наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 351. Компьютерный саботаж

Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.
2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, - наказывается лишением свободы на срок от трех до десяти лет.

Статья 352. Неправомерное завладение компьютерной информацией

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, - наказываются общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети - наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами - наказываются штрафом, или арестом на срок от трех до шести месяцев,

или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.
2. Те же действия, повлекшие тяжкие последствия, - наказываются лишением свободы на срок от трех до десяти лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.
2. То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.
3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3.3. Типы преступлений

Наиболее популярными ИТ-преступлениями являются следующие:

- Хищение денежных средств, используя украденные реквизиты банковских пластиковых карточек;
- «Нигерийские письма», «Лотерии», «Аукционы», «Брачные контракты», «Финансовые пирамиды»;
- Мобильные телефоны;
- Фишинг.

Приведем пример некоторых преступлений (согласно официального ресурса Управления К МВД РБ):

Нигерийские письма

Как правило, в данной корреспонденции рассказывается о том, что некто, являясь наследником крупного состояния, по каким либо причинам не может его получить, а поэтому просит о денежной помощи, обещая вернуть многократно больше. Алгоритм дальнейших действий понятен. К сожалению, среди нас есть еще те, кто хочет опровергнуть известную пословицу про сыр в мышеловке.

Письмо от «жены» бывшего диктатора Заира»:

Dear friend,

I am Mrs. Sese-seko widow of late President Mobutu Sese-seko of Zaire, now known as Democratic Republic of Congo (DRC). I am moved to write you this letter. This was in confidence considering my present circumstance and situation. I escaped along with my husband and two of our sons Alfred and Basher out of Democratic Republic of Congo (DRC) to Abidjan, Cote d'ivoire where my family and I settled, while we later moved to settled in Morroco where my husband later died of cancer disease.

I have deposited the sum Eighteen Million United State Dollars (US$ 18,000,000,00.) With a security company for safe keeping. What I want you to do is to indicate your interest that you can assist us in receiving the money on our behalf, so that I can introduce you to my son (Alfred) who has the out modalities for the claim of the said funds. I want you to assist in investing this money, but I will not want my identity revealed. I will also want to acquire real/landed properties and stock in multi-national companies and to engage in other safe and non-speculative investments as advise by your good self.

Yours sincerely, Mrs. Mariam M. Seseseko.

На самом деле, все вышеописанное является распространенным видом мошенничества, для совершения которого меняется лишь содержание.

В августе 2004 года на электронный почтовый ящик одного из жителей нашей столицы пришло письмо на английском языке, в котором предлагалось инвестировать деньги под какие-нибудь проекты. Белоруса заинтересовало предложение, поскольку он искал инвесторов для строительства торгового центра в Минске. Последний вступил в переписку с человеком, представившимся гражданином ЮАР – работником Министерства горнодобывающей промышленности. В ходе телефонных переговоров потерпевшему было предложено приехать в Лондон для заключения контракта. В столице Великобритании предприимчивого белоруса встретили на дорогой автомашине и отвезли в шикарно обставленное офисное помещение, которое злоумышленники представили гражданину Республики Беларусь как банк. Здесь и состоялось подписание контракта. Далее, минчанин в несколько этапов осуществил перечисление денежных средств на счета, предоставленные компаньонами. Надо ли говорить, что ни денег, ни новых знакомых, белорусский предприниматель больше не увидел.

Общая сумма ущерба от мошеннических действий в отношении незадачливого предпринимателя составила около 700 тысяч долларов США и более 30 тысяч английских фунтов.

Разновидность «нигерийских писем»

Лотерея	**Аукцион**	**Работа**	**Брачный контакт**
Открываете электронный ящик	На специальных сайтах проводятся	Речь идет о письмах с предложениями	Все, что для этой аферы требуется:

и с удивлением читаете письмо: «С радостью сообщаем, что Вы стали победителем нашей лотереи и выиграли главный приз – автомобиль! Для оформления расходов по доставке приза переведите такую-то сумму». Для убедительности высылаются всевозможные атрибуты, подтверждающие подлинность: фотография автомобиля, номер лицензии, свидетельство о регистрации и прочая сфабрикованная макулатура.	торги, в качестве лотов которых оказываются дорогостоящие вещи. Вы торгуетесь, посредством персонального банковского чека или чека почтового ведомства, оплачиваете товар и ждете его. В лучшем случае, вместо заказанных вами швейцарских часов, получите однодневные часы «желтой» сборки. А в худшем – ваши деньги растворятся в реальных карманах виртуальных мошенников.	«$200 в день», «$500 в день» за несложную законную работу в интернете. Потенциальным жертвам предлагается сделать выгодные капиталовложения или устроиться на высокооплачиваемую работу, перечислив мизерную сумму.	придуманное имя, несколько фотографий молодых и красивых славянок. Жулик тонко «обрабатывает» жертву, играя на слабостях человека. Виртуальный роман заканчивается тем, что жертва высылает деньги на оплату визы и билетов для «возлюбленной». Самое удивительное то, что даже спустя месяцы после обмана любовник с цветами продолжает выжидать свою подружку в аэропорту…