**ПЛАН-КОНСПЕКТ**

**профилактическая акция «Неделя кибербезопасности**

**«Безопасный Интернет»**

**Как защитить свои сбережения в виртуальном мире**

На протяжении текущего года в Республике Беларусь вновь наблюдается рост количества преступлений в сфере информационных технологий. Подавляющее большинство из них составляют хищения денежных средств путем завладения реквизитами банковских платежных карт – ст. 212 (хищение имущества путем модификации компьютерной информации) Уголовного кодекса Республики Беларусь.

**Мошенники в киберпространстве и как им противостоять!**

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя Ваши эмоции.

Например, злоумышленник связывается с держателем карточки посредством телефонного звонка или со взломанного аккаунта друга, родственника или знакомого в социальных сетях. В ходе звонка или переписки мошенник:

1. Описывает свою сложную жизненную ситуацию и просит помочь ему материально;
2. Представляется работником банка, «запугивает» ложной информацией о сомнительных операциях с банковской платежной карточкой (наличии заявки на кредит, блокировке счета или мошеннических атаках), и предлагает для сохранения оставшихся денежных средств перевести их на новый счет;
3. Представляется потенциальным покупателем товара, объявление о продаже которого было размещено держателем карточки в сети интернет (наиболее популярны платформы по продаже б/у вещей).

**Сценарии могут быть разными, а итог один: держатель карточки самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли.**

**Помните! Такие случаи не относятся к принципу «нулевой ответственности» держателя карточки, так как конфиденциальные данные злоумышленнику сообщил он сам.**

**Обращаем Ваше внимание, что телефонный номер мошенника может быть похож на телефонный номер Банка и отличаться одной или несколькими цифрами.**

**Иногда, действительно, требуется получение комментариев от держателя карточки по факту совершения операции, которая является сомнительной для Банка. В таком случае Банк направляет на телефонный номер клиента SMS-сообщение с просьбой перезвонить в Центр клиентской поддержки Банка.**

Обезопасить себя от данного типа мошенничества можно, соблюдая простые меры безопасности и проявляя разумную бдительность. Если ваш собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуем незамедлительно завершить диалог и самостоятельно обратиться в Банк по номеру, указанному на Вашей банковской карте.

**Не будьте излишне доверчивыми, не совершайте действий, которые способствуют передаче конфиденциальных данных третьим лицам!**

Вот несколько простых советов, соблюдение которых, позволит не стать жертвой злоумышленников:

1. Перед тем, как откликнуться на просьбу друга в социальной сети, созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (задайте другу вопрос, ответ на который знаете только вы оба);
2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в Банк по указанному на банковской карте или официальном сайте номерам;
3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от Банка - это повод уточнить ее достоверность и перезвонить в Банк;
4. Работники Банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему дистанционного банковского обслуживания (Интернет-банкинг, М-банкинг и другие). В такой ситуации немедленно прервите разговор и свяжитесь с Банком;
5. Никому и никогда не сообщайте данные своей карточки и всегда держите ее в поле зрения при совершении платежей;
6. Обязательно подключите 3D-secure и смс-оповещение;
7. Используйте только официальный сайт Банка для входа в систему Интернет-банкинга или официальное мобильное приложение;
8. Регулярно обновляйте пароли, используемые для входа в систему дистанционного банковского обслуживания, а также для подтверждения платежей;
9. В случае выявления действий по карточке, которые вами не совершались, необходимо оперативно обратится в Банк или самостоятельно заблокировать карточку в системе дистанционного банковского обслуживания.

**Рассмотрим самые распространенные схемы мошенничества сейчас:**

**1.«Звонок из Банка»**

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка. Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка. У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

**У вас просят конфиденциальные данные**

Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя». Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVС-код). Это нужно якобы «для сохранности ваших денег».

**Как мошенник пытается вас убедить**

* «*Мы звоним с официального номера, проверьте на сайте».*
* *«В целях конфиденциальности я включаю робота, который защитит ваши данные»* (вы слышите в трубке лёгкий шелест).
* Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
* Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
* Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

**Важно!** Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!

**2.«Потенциальный покупатель»**

Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

**Ссылка**

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

**QR-код**

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

**Важно!** Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

**Запомните!** Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

**3.«Сообщения в социальных сетях»**

Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям. Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.

**Важно!**При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

**4.«Розыгрыши/раздачи/опросы от Банка или иных организаций»**

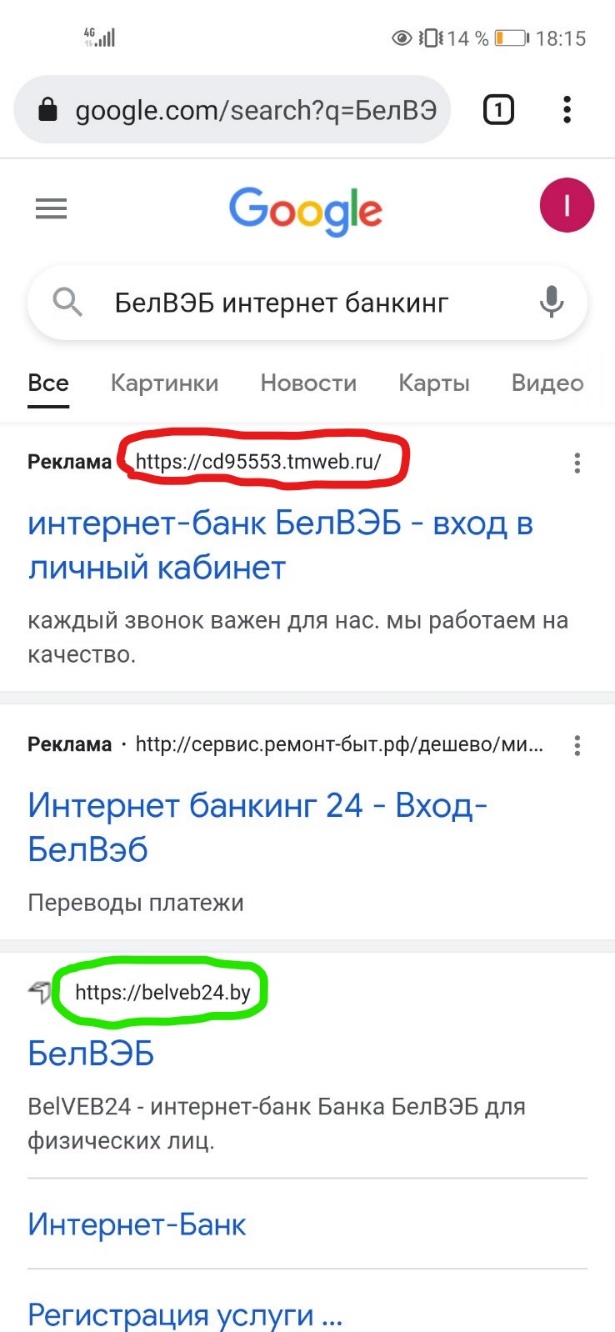
Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи я годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение. Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения либо с целью получения последнего – ввести данные Вашей банковской карты. Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

**Важно!** Посетите официальную страницу организации или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.

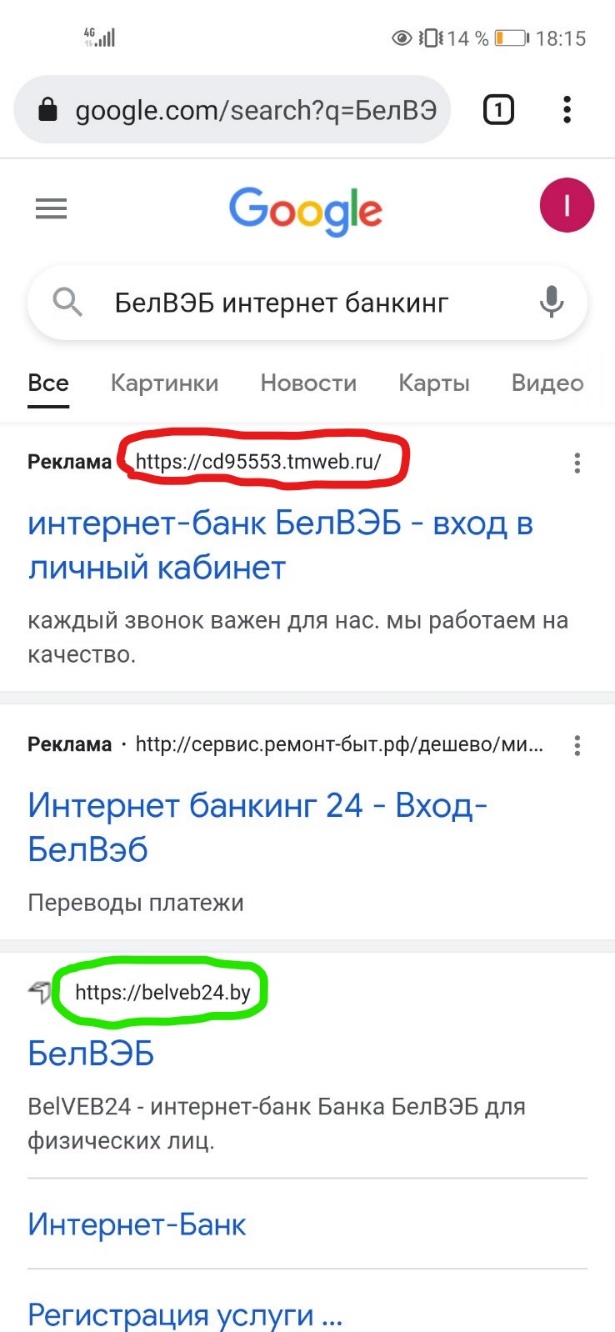
**5.«Фишинг - поддельные сайты банковских учреждений»**

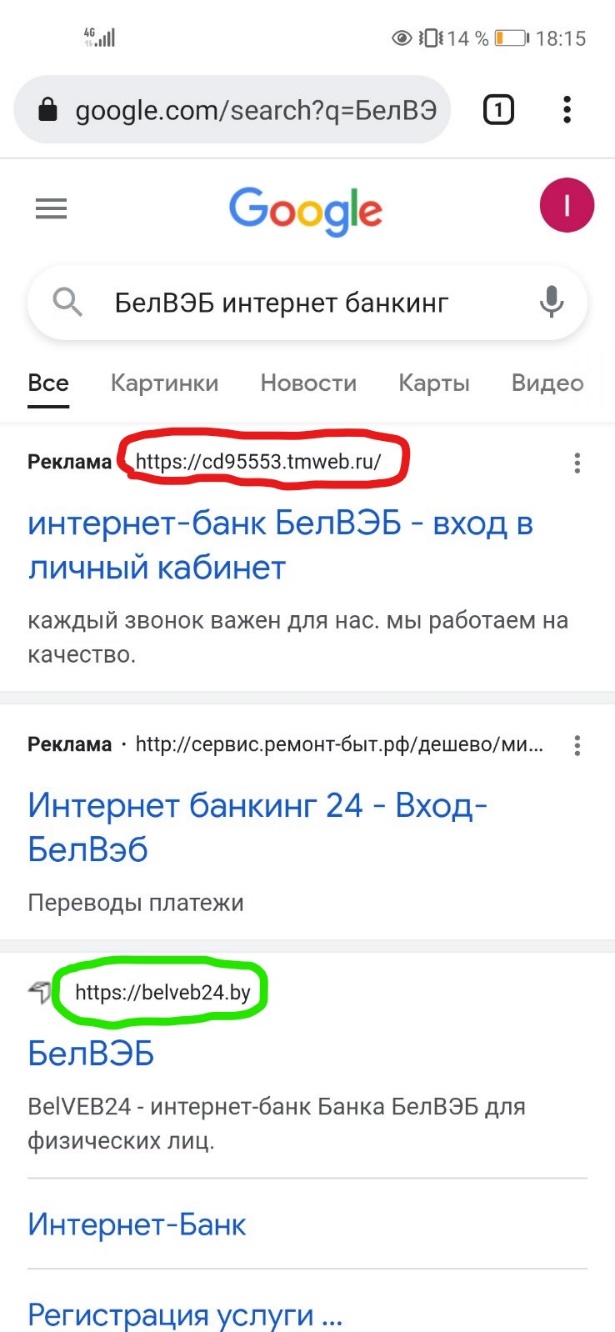
Если Вы используете систему дистанционного банковского обслуживания «Интернет-банкинг» для расчетов за коммунальные услуги, денежных переводов, проверки факта зачисления на счет заработной платы (пенсий, пособий и т.п.), Вам необходимо удостовериться в подлинности веб-ссылки, предназначенной для авторизации на интернет-сайте банка.

Дело в том, что кибермошенники временно размещают в сети Интернет веб-ссылки, которые ведут на поддельные (фишинговые) веб-сайты, внешне не отличающиеся от оригинальных.



Пример «фишинговой» ссылки на интернет-банкинг, обнаруженной в результате поискового запроса в браузере «Google».



Подлинная ссылка на веб-сайт интернет-банкинга «Банк БелВЭБ», обнаруженная в результате того же поискового запроса в браузере «Google».

В случае перехода на поддельный веб-сайт, Вам будет предложено ввести «логин» и «пароль» для авторизации. Если Вы это сделаете, то киберпреступники получат доступ к Вашему интернет-банкингу, а находящиеся на банковском счету денежные средства будут похищены. Также Вам не следует переходить по ссылкам, которые Вы получили от неизвестных людей в социальных сетях или мессенджерах. С большой долей вероятности, данные ссылки являются «фишинговыми».

Для безопасного совершения онлайн платежей рекомендуется использовать специальные приложения для мобильных устройств «Мобильный банкинг», которые доступны для скачивания в Google Play Market (для Android) или App Store (для iOS).

**Кто такие дропы?**

Дропы помогают преступникам «отмывать» нелегально полученные деньги. Например, деньги, добытые путем совершения киберпреступлений в сфере электронной коммерции и платежных операций (фишинг, вишинг, смишинг).

Дропы также могут быть вовлечены в схемы отмывания денег, добытых другими преступными путями: торговлей наркотиками, торговлей людьми и др.

Дроп или «денежный мул» – этот тот человек, который соглашается, чтобы его банковская карта стала «транзитной» для украденных мошенниками денег. Дроп переводит незаконно полученные денежные средства между разными счетами. Такая цепочка переводов нужна для того, чтобы запутать следы киберпреступников и усложнить работу следствия.

Дропы могут совершать переводы в разных странах и от имени разных людей. Таким образом, преступные синдикаты легко перемещают средства по всему миру, оставаясь «невидимыми».

Дроп не всегда осознает, что вовлечет в преступную схему. Мошенники часто маскируют свои действия под «легальный бизнес».

Дропа привлекают к сотрудничеству, обещая «золотые горы», – быстрый и легкий способ заработать много денег. За свое сотрудничество с преступниками «денежный мул» получает процент от сумм, которые помогает «отмывать».

Дроп – это «низшее» звено преступной сети, на которое правоохранители выходят в первую очередь.   
 Дроп – правонарушитель, соучастник преступления.

Дроп – тот, кто за свои преступления получает строгий приговор: штрафы, конфискацию имущества, лишение свободы.

**Кто становится дропом?**

Группа риска – люди, у которых шаткое материальное положение:

Переехавшие в большой город из маленького;

Безработные; Студенты и учащиеся;

Представители экономически и социально уязвимых групп населения (многодетные семьи, сироты и т.д.).

Независимо от того, какие причины стали поводом для выбора работы дропом – наказание все равно наступит. Незнание законов не освобождает от ответственности!

**Как отличить предложение стать дропом от прочих предложений о работе:**

В описании работы указано, что необходимо переводить деньги;

Не описаны конкретные профессиональные требования к соискателю работы, нет перечня его обязанностей, кроме перевода денег;

Отсутствуют требования относительно образования и уже имеющегося опыта работы соискателя;

Работа предполагает только онлайн-взаимодействие с работодателем (без личного общения);

Предложение о работе чрезвычайно выгодное: мало усилий, – большие заработки. Некоторые объявления предлагают потратить в день около 10 минут, чтобы зарабатывать в месяц до 1000 рублей.

**Обратите внимание!**

Объявления о вербовке дропом могут быть замаскированы под предложения о работе от реальных компаний. Создаются целые поддельные сайты, похожие на официальные веб-ресурсы реально существующих компаний.

Мошенники выдумывают «уважительные» причины, по которым им нужно переводить деньги с одного счета на другой. Самая распространенная причина – уклонение от налогов. Дропов вербуют  
 от имени некой компании, которой, якобы, нужно минимизировать налоговые выплаты (и для этого следует переводить часть дохода через счета физических лиц).

Предложение о работе может поступить и в виде письма на электронную почту. Обратите внимание на адресата: если он предлагает работу от лица компании, но при этом в адресе отправителя письма не указан домен компании (а указана веб-служба, например, Gmail, Yahoo, Windows Live Hotmail и др.), это может быть признаком вербовки дропов.

**Запомните основные признаки ловушек для дропов:**

Если предложение о работе выглядит слишком заманчивым, чтобы быть правдой, – значит, это ловушка!

Если вас уверяют, что можно заработать большие деньги, прилагая минимум усилий, – значит, это ловушка!

Если для получения работы вам нужно предоставить свою банковскую карту – значит, это ловушка!

Если вам предлагают работу от компании, о которой нет никакой информации в Интернет, – значит, это ловушка!

Если на официальном сайте компании, которая, якобы, предлагает вам работу, нет ни слова о вакансиях и о работе, включающей перевод денег (и об этом даже не слышали в отделе кадров компании) – значит, это ловушка!

Если супервыгодное предложение о работе поступило через социальные сети или электронную почту, а отправитель вам незнаком - значит это ловушка!

В мессенджере «Telegram» можно найти различные телеграм-каналы (например: «Дроп и дроповоды»), в которых содержаться объявления о заработке, связанные с банковскими карточками, именно там ищут людей, которые на свое имя оформляют карточки для их последующего использования в преступных схемах.

Граждане по просьбе знакомых или за вознаграждение открывают на свое имя счета в банках. Оформляют банковские платежные карты, пользоваться которыми не собирались, и в нарушение условий договора с банком передают реквизиты другим людям. Злоумышленники использовали карты для перевода, легализации и обналичивания денег, которые получили от преступных сделок.

Особое беспокойство вызывает то, что в данную преступную схему вовлекают подростков, которые даже не осознают противоправности своих действий. Достигнув возраста 14 лет, подросток может самостоятельно оформить банковскую платежную карточку на свой паспорт. Для открытия счета даже не требуется приходить в банк – все можно сделать онлайн. С использованием мобильных приложений различных банков они открывают счета, регистрируют электронные кошельки, а затем сообщают злоумышленникам все данные и реквизиты.

Были случаи, когда подростки, получив вознаграждение, по просьбе мошенников подыскивали среди товарищей тех, кто согласится оказать такую же «услугу», получая за это дополнительную плату.

*Ответственность за изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, предусмотрена ст. 222 УК Республики Беларусь.*

***Статья 222 УК Республики Беларусь. Изготовление либо сбыт поддельных платежных средств.***

1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, – наказываются штрафом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, – наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

Ответственность за совершение преступления, предусмотренного  
ст. 222 УК Республики Беларусь наступает с 16 лет.

***Статья 212*** ***УК Республики Беларусь.*** ***Хищение имущества путем модификации компьютерной информации.***

1.Хищение имущества путем модификации компьютерной информации наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, 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, – наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или 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 1 или 2 настоящей статьи, совершенные в крупном размере, – наказываются ограничением свободы на срок от двух до пяти лет или лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере, –наказываются лишением свободы на срок от пяти до двенадцати лет со штрафом и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Ответственность за совершение преступления, предусмотренного  
ст. 212 УК Республики Беларусь наступает с 14 лет.