МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

УПРАВЛЕНИЕ ВНУТРЕННИХ ДЕЛ ГРОДНЕНСКОГО ОБЛИСПОЛКОМА

КРИМИНАЛЬНАЯ МИЛИЦИЯ

ОТДЕЛ ПО РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

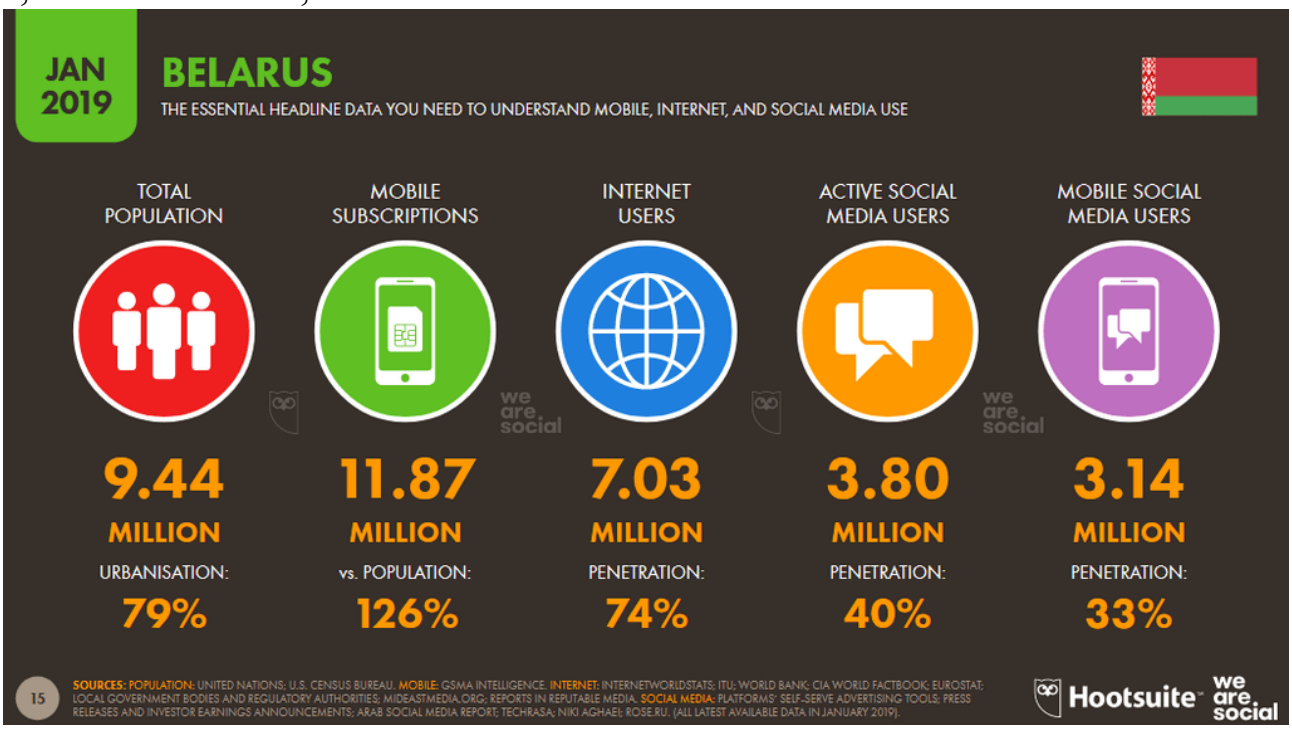
ПЛАН КОНСПЕКТ

Тема: «Профилактика наиболее распространенных видов преступлений против информационной безопасности»

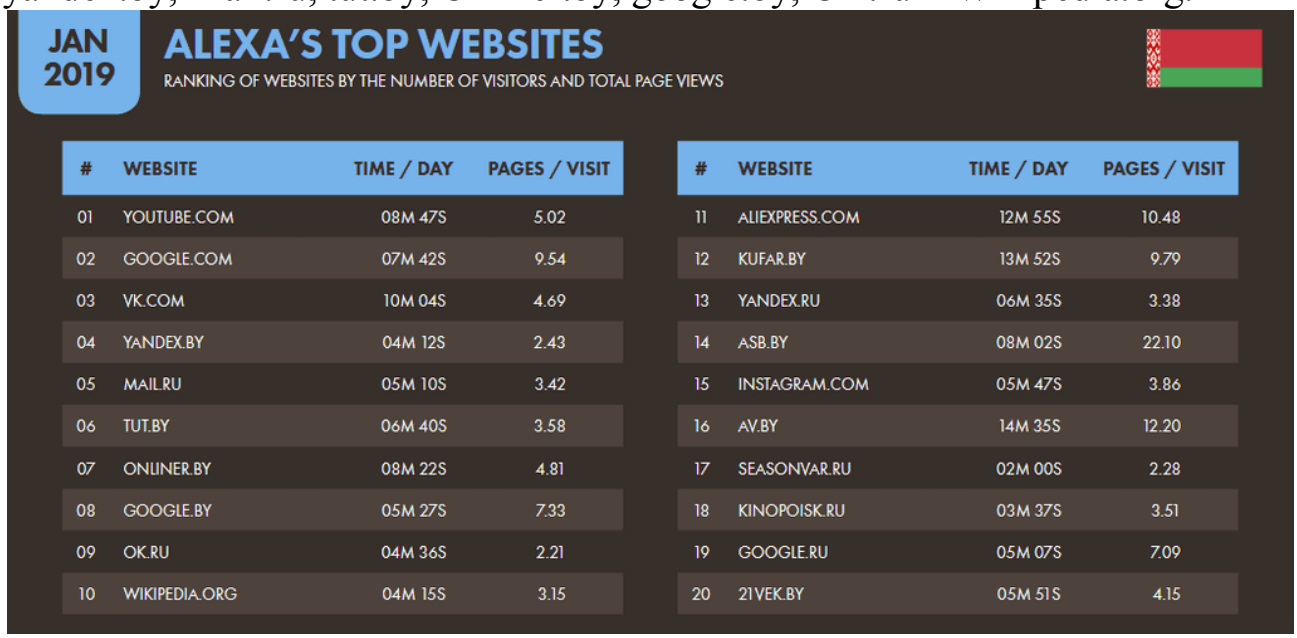
г. Гродно
2019

Количество пользователей сети интернет в Республике Беларусь и их сетевая активность имеют устойчивую тенденцию роста. Приведем некоторые статистические данные из открытых источников сети интернет.

К январю 2019 года на 9,44 млн. жителей Беларуси приходилось 11,87 млн. абонентов мобильной связи, за год прирост составил 3,1%. Количество интернет-пользователей также показало рост 4,5% и равняется 7,03 млн. человек, или 74% населения.



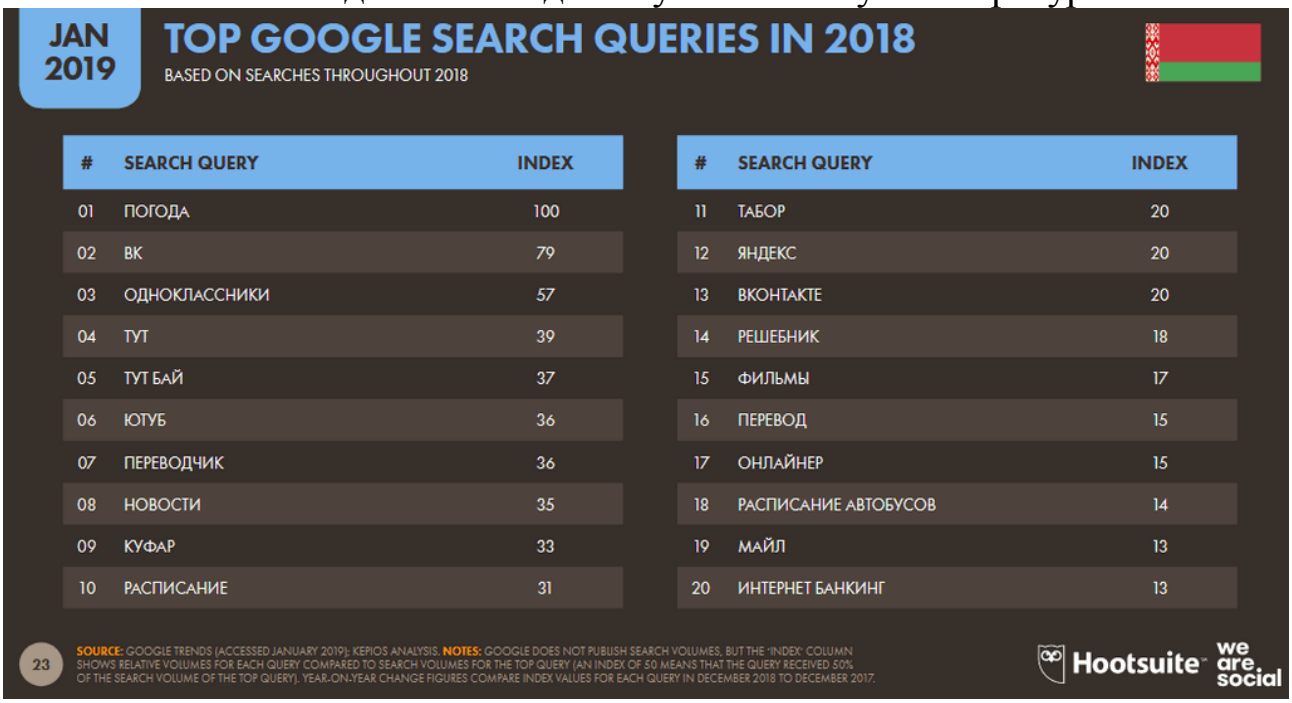
Самым популярным сайтом является YouTube, в среднем в день пользователь проводит на нём примерно 8 минут 47 секунд. На втором месте google.com – 7 минут 42 секунды, на третьем – сайт соцсети «ВКонтакте» с результатом 10 минут 4 секунды. В топ-10 попали yandex.by, Mail.ru, tut.by, Onliner.by, google.by, OK.ru и Wikipedia.org.



#	WEBSITE	TIME / DAY	PAGES / VISIT
01	YOUTUBE.COM	08M 47S	5.02
02	GOOGLE.COM	07M 42S	9.54
03	VK.COM	10M 04S	4.69
04	YANDEX.BY	04M 12S	2.43
05	MAIL.RU	05M 10S	3.42
06	TUT.BY	06M 40S	3.58
07	ONLINER.BY	08M 22S	4.81
08	GOOGLE.BY	05M 27S	7.33
09	OK.RU	04M 36S	2.21
10	WIKIPEDIA.ORG	04M 15S	3.15

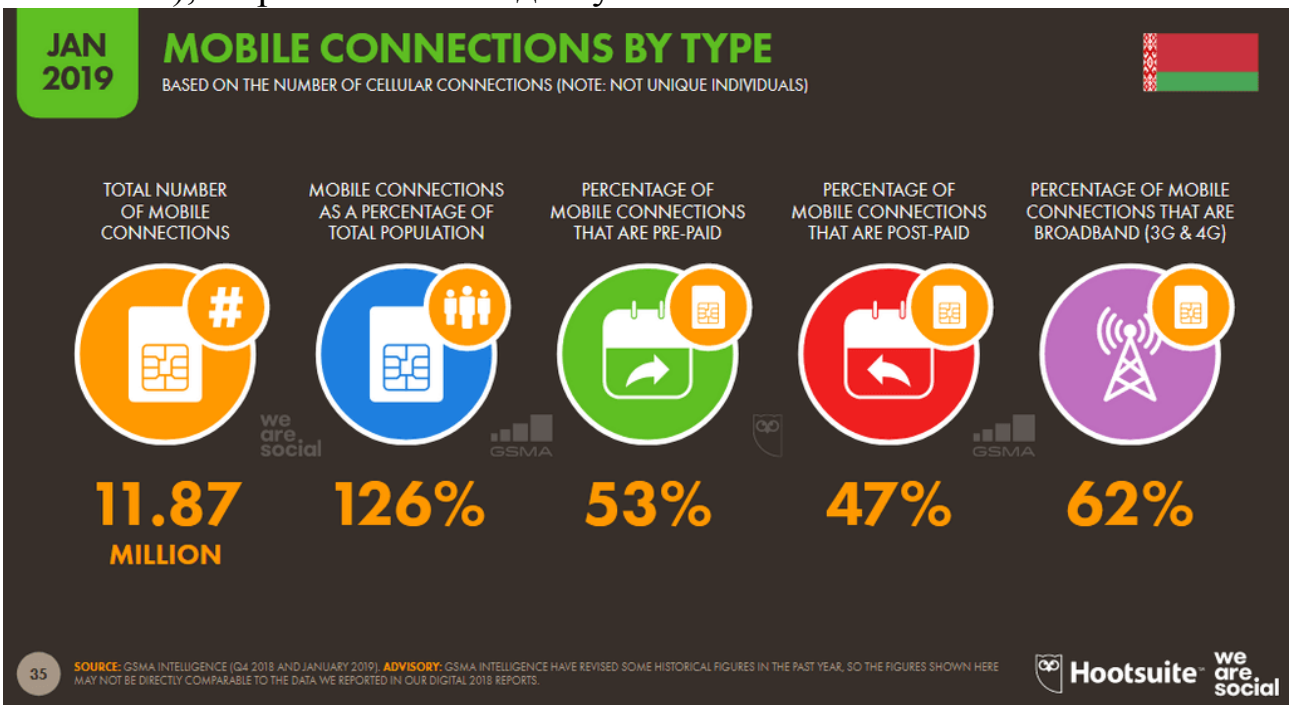
#	WEBSITE	TIME / DAY	PAGES / VISIT
11	ALIEXPRESS.COM	12M 55S	10.48
12	KUFAR.BY	13M 52S	9.79
13	YANDEX.RU	06M 35S	3.38
14	ASB.BY	08M 02S	22.10
15	INSTAGRAM.COM	05M 47S	3.86
16	AV.BY	14M 35S	12.20
17	SEASONVAR.RU	02M 00S	2.28
18	KINOPOISK.RU	03M 37S	3.51
19	GOOGLE.RU	05M 07S	7.09
20	21VEK.BY	05M 51S	4.15

Топовым поисковым запросом Google в 2018 году была «погода». Несколько реже белорусы искали «вк» и «одноклассники». При этом специфика поисковых запросов показывает, что пользователи не запоминают адреса полюбившихся сайтов, а ищут их в поисковике, что может повлечь попадание на подложную копию нужного ресурса.



Активные пользователи соцсетей составили 3,8 млн. человек, из них почти 83 процента пользуются соцсетями с мобильных устройств. Например, количество белорусских посетителей ВКонтакте оценивается в 3,5 млн., Одноклассников – около 2,7 млн., рекламная аудитория Instagram составляет 2,1 млн. пользователей, Facebook – 1 млн.

В Беларуси около 11,87 млн. мобильных абонентов (126% населения), широкополосный доступ имеют 62% абонентов.



Согласно исследованиям, 81% белорусов имеет счёт в банке, 46% делают покупки или оплачивают счета через интернет. Количество выданных банковских платежных карточек на конец 2018 года по данным Национального банка Республики Беларусь превысило 15 млн., инфраструктура их обслуживания включает более 121 тыс. объектов торговли и сервиса, более 4200 банкоматов, 3100 инфокиосков.

Указанные темпы проникновения информационных технологий и безналичных платежей во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью и неосмотрительностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

В законодательстве Республики Беларусь предусмотрена ответственность, в том числе уголовная за совершение противоправных деяний в сфере высоких технологий.

Уголовным кодексом предусмотрен ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

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, 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 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 лишением свободы на срок от двух до семи лет со штрафом или без штрафа с конфискацией имущества или без конфискации 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 шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Необходимо отметить, что ответственность за деяния, предусмотренные *ст.212*, наступает *с 14-летнего возраста*.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. В последнее время наиболее актуальны факты хищений с использованием реквизитов карт при осуществлении интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

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 (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, -

наказывается штрафом или арестом.

2. Несанкционированный доступ к компьютерной информации, совершенный 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, 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.

Например – несанкционированный доступ (открытие и просмотр файлов, писем, переписки) к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

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, 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 3 статьи 349 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.

В качестве примера можно привести произведенные изменения компьютерной информации: переписка в электронной почте, в социальной сети, в мессенджере с правами другого пользователя; изменение текстовой, графической и иной информации; внесение изменений в защищенные базы данных и т.д.

Статья 351. Компьютерный саботаж

1. 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, 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.

Здесь мы говорим об умышленном уничтожении (удалении, приведении в непригодное состояние, шифровании) компьютерной информации либо ее блокировании (например путем смены пароля доступа, изменении графического ключа и т.д.).

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, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации, повлекшие причинение существенного вреда. К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами фотографий с компьютера.

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, или ограничением свободы на срок до двух лет.

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов, например поддельных смарт-карт для просмотра закодированных каналов спутникового телевидения.

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, 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.

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

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.

Указанная статья может быть применена к лицам, имеющим доступ к компьютерным сетям и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем.

Ответственность за деяния, предусмотренные *ст.ст.349-355,* наступает *с 16-летнего возраста*.

Также с использованием сети Интернет может совершаться ряд иных уголовно наказуемых противоправных деяний:

– мошенничество (ст.209 УК);

– причинение имущественного ущерба без признаков хищения (ст.216 УК);

– изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343 УК, ст.343-1 УК);

– клевета (ст.188 УК);

– оскорбление (ст.189 УК);

– разжигание расовой, национальной или религиозной вражды или розни (ст.130 УК) и иные.

В результате работы, направленной на выявление и раскрытие преступлений указанной категории на территории Гродненской области, в 2018 году были достигнуты следующие результаты. Зарегистрировано 300 (+34 к прошлому году или +12,8%) преступлений в сфере высоких технологий, в том числе 211 (+34, +19,2%) – по ст.212 УК, 89 (+/-) – преступления против информационной безопасности (67 – по ст.349 УК, 3 – ст.350 УК, 15 – ст.351 УК, 2 – ст.352 УК, 2 – ст.354 УК). Удельный вес преступлений в сфере высоких технологий, по которым установлен подозреваемый и производство по которым окончено в Гродненской области составил 50,2% при среднереспубликанском показателе 42,8%.

По оконченным производством уголовным делам выявлен материальный ущерб в сумме более 41 тысячи рублей, 75% которого возмещено на стадии следствия.

За совершение преступлений в сфере высоких технологий к уголовной ответственности привлечено 106 лиц, из них 2 несовершеннолетних, 30 женщин, 31 – ранее судимых.

Два месяца 2019 года показывают, что активный рост киберпреступности продолжается. Зарегистрировано 138 преступлений, что почти в 2,5 раза выше показателя аналогичного периода прошлого года, из них 77 (рост более чем в 2 раза) – хищения с карт-счетов и 61 –

преступления против информационной безопасности. По всем фактам хищений установлен имущественный ущерб в сумме 40,8 тыс. рублей или в среднем 305 рублей на 1 преступление.

Необходимо отметить, что преступность в сфере высоких технологий характеризуется высокой степенью латентности, в результате чего реальное количество киберинцидентов существенно выше.

В 2018 и начале 2019 года на территории Гродненской области наблюдается отчетливая тенденция роста количества фактов совершения противоправных деяний в сети Интернет, которые выражаются, с одной стороны, во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, а с другой стороны – в совершении хищений с карт-счетов граждан путем использования компьютерной техники либо мошенничества. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет и некоторым несовершенством банковских инструментов. Согласно проведенного анализа такие преступления в 2019 году составляют около 84% от общего числа всех возбужденных дел по линии высоких технологий.

Сначала преступник получает несанкционированный доступ к средству связи с потенциальным потерпевшим, обычно это учетные записи в социальных сетях ВКонтакте, Одноклассники, электронные почтовые ящики, аккаунты в различных программах, предназначенных для обмена сообщениями, например Skype. Чаще всего это становится возможным ввиду небрежного отношение владельца сайта к обеспечению сохранности конфиденциальной информации (логинов, паролей) о пользователях либо беспечности самих пользователей. При этом такая беспечность со стороны пользователей может проявляться в:

– попадании на удочку лиц, создавших «фишинговый» (имитирующий настоящий) сайт;

– вводе логинов и паролей от своих учетных записей в соцсети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах;

– использовании идентичных реквизитов для авторизации на различных ресурсах;

– использовании слишком легких паролей;

– установке непроверенного программного обеспечения, предлагаемого на различных сайтах, в том числе, когда такие приложения требуют ввод

платежных реквизитов, учетных данных электронной почты или аккаунта в соцсети;

– отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ и др.

Получив реквизиты, злоумышленник заходит в учетную запись жертвы и осуществляет рассылку контактам владельца взломанной учетной записи сообщений мошеннического характера.

Следует констатировать, что фантазия преступников безгранична, вариантов формулировок таких просьб множество, приведем некоторые примеры таких сообщений:

– «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом переведешь мне, когда мою карту разблокируют. В долгу не останусь!»;

– «Доброго времени суток! Какого банка у тебя карточка? Именно этого мне и нужна, чтобы избежать комиссии. Можешь дать реквизиты или сфотографировать? Там еще на обратной стороне три цифры есть. Тебе на телефон должен придти код, напиши сюда. Нет, не беспокойся, твои деньги никуда не денутся.»;

– «Можешь дать логин и пароль от интернет-банкинга. В моем выдает какую-то ошибку, хочу проверить, есть ли в твоем такой баг. Платежей делать не буду, мы же друзья!»

– «Привет, друг, я нахожусь в России, у меня украли кошелек и телефон. Срочно нужны деньги на билет домой. Отправь мне на карт-счет (мобильный номер телефона, кошелёк в электронных платежных системах Яндекс.Деньги, QIWI, WebMoney или других) определенную сумму. По приезду все верну»;

– «Я помогаю в сборе средств для лечения моей дальней родственницы, у нее серьезная болезнь, нужно много денег. Перечисли, если есть возможность, хоть какую-то сумму на кошелек».

Далее преступнику остается ждать отклика от ничего не подозревающих собеседников и проявлять свои способности в риторике и убеждении.

В случае, когда потерпевший отзывается на уловку преступника и, будучи обманутым, сам осуществляет перевод средств на предложенные реквизиты, в действиях злоумышленника усматривается состав преступления, предусмотренного статьей 209 Уголовного кодекса Республики Беларусь «Мошенничество» (в зависимости от суммы похищенного максимальная ответственность может составлять как три, так и десять лет лишения свободы).

Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение путем использования компьютерной техники» (также в зависимости от суммы максимальное наказание варьируется от 3 до 15 лет лишения свободы, при этом Законом не предусмотрена минимальная сумма хищения). В данном случае под реквизитами карты необходимо понимать:

– 16-значный номер карты, срок действия, имя владельца (эти данные указаны на лицевой стороне карты), обычно 3-значный CVC-код с обратной стороны карты, код подтверждения транзакции 3D-Secure (может задаваться пользователем либо формироваться процессинговым центром и направляться на мобильный номер владельца карты посредством SMS или push-уведомления);

– логин и пароль доступа к системе дистанционного банковского обслуживания (интернет-банкинга), а также код подтверждения доступа с карты кодов либо динамический код, направленный на мобильный номер владельца карты посредством SMS или push-уведомления.

Наличие у третьих лиц указанной выше информации позволяет им совершать расходные операции в сети Интернет, например перевод средств на другие карты, приобретение электронных денег, оплату товаров и услуг в пределах баланса карточки. В некоторых случаях доступ в интернет-банкинг позволяет распоряжаться депозитами клиента и оформлять заявки на получение кредитов.

Необходимо отметить, что совершение транзакций по банковским платежным карточкам самим владельцем либо нарушение правил пользования карточками, выразившееся в передаче платежных реквизитов третьим лицам, практически не оставляет шансов вернуть денежные средства с использованием действующего в Беларуси принципа нулевой ответственности пользователей банковских карточек.

Учитывая изложенные выше факты, приведем некоторые рекомендации для пользователей сети интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

– для выхода в сеть интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;

– используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения, скачанные из официальных магазинов приложений;

– при использовании известных Вам сайтов, обращайте внимание на их внешний вид и адрес: возможно Вы зашли на поддельную его копию;

– вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);
– не используйте одинаковые логины и пароли на различных сайтах;
– не используйте слишком легкие пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т.д.), периодически изменяйте свои пароли;
– по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;
– остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;
– с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным интернет-каналам;
– при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь), либо в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;
– не храните реквизиты карты в открытом доступе, в том числе в виде фотографий, не передавайте карту третьим лицам;
– если Вы не используете банковскую платежную карточку для осуществления интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;
– используйте для платежей в сети интернет специализированные карточные продукты с отдельным счетом, обязательно подключите SMS-информирование о совершении расходных транзакций;
– при осуществлении интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ;
– в случае получения информации о несанкционированном списании средств с карточки незамедлительно принимайте меры к ее блокировке путем обращения в службу поддержки банка по телефону либо через

интернет-банкинг, а также обращайтесь в банк с целью инициирования процедуры опротестования мошеннических транзакций, а также рассмотрения возможности возврата денежных средств в соответствии с принципом нулевой ответственности.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но в общем можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к происходящему в сети интернет.

В случае совершения в отношении Вас противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства либо обнаружения факта совершения преступления.

Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!

ОРПСВТ КМ УВД Гродненского облисполкома