ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ.

Информационная безопасность является понятием многогранным и комплексным. Она имеет два основных аспекта: содержательный (духовная сфера) и технический (материальная сфера). К первому из них можно отнести содержание и направленность информации. Технический аспект - совокупность информационно-телекоммуникационных средств, технологий, систем, ресурсов, предназначенных для создания, хранения, распространения, передачи и обработки информации.

18 марта 2019 года опубликована Концепция информационной безопасности Беларуси. Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности. Большое внимание в концепции уделено и вопросам обеспечения безопасности информационной инфраструктуры, в том числе национального сегмента сети интернет, противодействию киберпреступности.

Киберпреступление — вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации, например информации по банковским счетам. Киберпреступлениями считаются те преступления, в которых ведущую роль играют компьютер или компьютерная сеть.

Статистика

Состояние криминогенной обстановки по направлению деятельности подразделений в сфере высоких технологий в январе – июне т. г. в сравнении с аналогичным периодом прошлого года (далее – 2019 и 2020 гг. соответственно) свидетельствует об увеличении (+15,6%; с 4 049 до 4 679) количества зарегистрированных киберпреступлений.

- 2019 г. - 2020 г.

При этом число выявленных подразделениями МВД уголовно наказуемых деяний увеличилось во всех регионах, за исключением Брестской (-6,0%; с 514 до 483) области, наиболее значительно в Гродненской (+39,5%; с 392 до 547), Витебской (+33,8%; с 438 до 586) и Могилевской (+26,8%; с 410 до 520) областях.*

(* информация с сайта https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/statistika-urpsvt)

В результате проведенных оперативно-розыскных мероприятий установлено в 2019 году 1 859 лиц (2018 г. - 1 283) виновных в совершении преступлений. К уголовной ответственности привлечено 1 431 (2018 г. - 1 139) граждан, в т. ч. 524 (2018 г. - 369), имеющих судимость, 1 177 (2018 г. - 849) неработающих и неучащихся, 77 несовершеннолетних (2018 г. - 35).*

(* информация с сайта https://www.interfax.by).

Статья 212 УК РБ. 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, ши лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом, ши 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 ши без штрафа и с лишением права занимать определенные должности ши зангшатъся 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 ши заниматься определенной деятельностью ши без лишения.

Самым распространённым примером, встречающимся в отношении преступлений, предусмотренных статьей 212 УК РБ является ввод преступником персонифицированного идентификационного номера (ПИН-кода) чужой пластиковой банковской карточки, т.к. в данном случае хищение происходит

посредством компьютерной техники у потерпевшего, который не давал разрешения на производство операций с его банковской карточкой.

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 ши 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, ши лишением права занимать определенные должности или заниматься определенной деятельностью, ши арестом, ши ограничением свободы на срок до двух лет, ши 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 ши лишением свободы на срок до семи лет.

Ответственность за деяния, предусмотренные ст.212, наступает с 14- летнего возраста, ст. 349 — с 16-летнего возраста.

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;
- ✓ при использовании известных Вам сайтов, обращайте внимание на их внешний вид: 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.);
- ✓ 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;
- ✓ если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;
- ✓ 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.

ПРОЯВЛЯЙТЕ БДИТЕЛЬНОСТЬ И КРИТИЧЕСКОЕ ОТНОШЕНИЕ К ОКРУЖАЮЩИМ НАС СОБЫТИЯМ