**Информационное сообщение**

о проведении информационной встречи в трудовом коллективе ГУО «Средняя школа № 6 г. Светлогорска»

Дата проведения: «15» декабря 2022 года

Место проведения: ГУО «Средняя школа № 6 г. Светлогорска», актовый зал

Тема: Основные направления государственной политики в области информационной безопасности.

Количество присутствующих: 30 человек

Встречу провели (ФИО, должность): Киселева Н.Г., директор школы, Савенко О.А., заместитель директора по учебной работе, Кривопуск И.А., заместитель директора по воспитательной работе

**Критические замечания, предложения, просьбы, вопросы, поступившие в ходе встречи** **(всего)** \_\_\_\_\_1\_\_\_

1.Вопросы, ответы на которые даны в ходе встречи (всего): \_\_\_\_1\_\_\_\_

1 вопрос: Преступления в сфере высоких технологий и защита от них.

Ответ: За сравнительно небольшой промежуток времени количество пользователей сети Интернет в Республике Беларусь превысило пять миллионов человек. Сегодня по плотности проникновения широкополосного доступа на 100 человек Беларусь вышла на среднеевропейские показатели, а по скорости – на третье место в мире. Количество абонентов сотовой связи продолжает увеличиваться. Указанные темпы проникновения информационных технологий во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью 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

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 все чаще фиксируются 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

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

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

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

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

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

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

Указанная статья применяется 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.

2.Вопросы, решение которых поставлено на контроль (всего): 0

3.Вопросы, волнующие работников трудового коллектива:

1 вопрос: Меры наказания за преступления в сфере высоких технологий?

Ответ: В уголовном праве Беларуси закреплена ответственность за ряд преступлений против информационной безопасности (Глава 31 УК РБ):

Статья 349. Несанкционированный доступ к компьютерной информации. Наказание: штраф, арест, ограничение или лишение свободы на срок до 2 лет. Если действия, предусмотренные статьей, повлекли тяжкие последствия – возможно ограничение свободы на срок до 5 лет или лишением свободы на срок до 7 лет.

Статья 350. Модификация компьютерной информации. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет.

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. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, арест, ограничение свободы на срок до 5 лет, лишение свободы на срок 3-10 лет.

Статья 352. Неправомерное завладение компьютерной информацией наказывается общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением или лишением свободы на срок до 2 лет.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети наказывается штрафом, или арестом на срок 3-6 месяцев, или ограничением свободы на срок до 2 лет.

Статья 354. Разработка, использование либо распространение вредоносных программ. Наказание: штраф, арест, ограничение свободы на срок до 2 лет, лишение свободы до 10 лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети. Наказание: штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, исправительные работы на срок до 2 лет, ограничение свободы на срок до 5 лет, лишение свободы на срок до 7 лет.

Дата: «15» декабря 2022 год

Подпись руководителя информационной группы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_