МАТЕРИАЛЫ
для членов информационно-пропагандистских групп
Минской области (ноябрь 2024 г.)

Кибербезопасность и профилактика киберпреступности и мошенничеств, совершаемых с использованием информационно-коммуникационных технологий

Стремительное развитие цифровых технологий, переход к безналичным расчетам, размещение в глобальной компьютерной сети Интернет персональных данных при достаточно низкой цифровой грамотности граждан, сопряженной с беспечным отношением к защите собственной информации, стали следствием увеличения количества регистрируемых киберпреступлений.

Злоумышленники активно используют в своей деятельности новейшие достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационные технологии для совершения и сокрытия преступлений.

По итогам десяти месяцев 2024 года, в сравнении с аналогичным периодом прошлого года (далее – АППГ), количество зарегистрированных киберпреступлений на территории Минской области увеличилось на **21,9 % (с 1603 до 1954),** что является **каждым пятым (20,3 %) уголовным делом на Минщине**. Число тяжких киберпреступлений возросло **в 0,8 раз (с 125 до 228, или на 82,4 %)**.

Вместе с тем, на фоне роста зарегистрированных киберпреступлений, уровень раскрываемости увеличился с **17,7 %** до **19,1 %**.

Необходимо отметить, что если в предыдущие периоды большинство киберпреступлений, относились к хищениям имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса),
то в текущем году в связи с отнесением к компетенции подразделений по противодействию киберпреступности (далее – ПК) мошенничеств и вымогательств, совершенных с использованием информационно-коммуникационных технологий, тенденция изменилась.

Так, в январе-октябре 2024 года совершено **1123** мошенничеств (ст. 209 Уголовного кодекса) (АППГ – 78), или **57,5 %**, от общего числа зарегистрированных киберпреступлений.

Структурный анализ совершенных в текущем году мошенничеств свидетельствует о явном преобладании таких способов завладения деньгами потерпевших, как:

1. Продажа несуществующего товара, на различных Интернет-ресурсах.

Очень часто жертвами мошенников становятся пользователи сети Интернет, желающие приобрести различные товары в социальной сети **Instagram – 483 преступления, или 43 %**. Продавцы, как правило, просят предоплату за товар, однако такие истории заканчиваются одним – граждане перечисляют предоплату, а в дальнейшем связь с продавцом теряется, не получив долгожданный товар.

Для примера можно рассмотреть следующие мошеннические учетные записи: **easy_step_by, original_brand.by, edelweis.resort, fox.store.by, EUROSHINA_BY, @airmac_by, flowerslovers.by, _belbet_off, happysale.by**.

2. Обман граждан под предлогом вложения средств в криптовалюту либо сделок с ней на несуществующих биржах и иного заработка в сети Интернет 135 преступлений, или 12 %.

Несуществующие инвестиционные проекты и мошеннические биржи — это обманные схемы, в которых инвесторам предлагается вложить средства в вымышленные или несуществующие бизнес-проекты, или финансовые инструменты с обещаниями высокой прибыли, которая на самом деле не может быть достигнута.

Мошеннические биржи, предлагающие несуществующие инвестиционные проекты, обычно используют различные хитрости и тактики, чтобы привлечь потенциальных инвесторов. Вот несколько типичных характеристик таких мошеннических схем:

1. Обещания высокой доходности при минимальных рисках: Мошеннические биржи обычно привлекают внимание инвесторов, обещая очень высокие доходы при минимальном или даже отсутствующем риске. Это является привлекательным для людей, желающих получить быструю и легкую прибыль, однако на самом деле такие обещания часто оказываются ложными.

2. Неясные условия инвестирования и вывода средств: Мошеннические биржи часто предлагают инвесторам неясные и запутанные условия инвестирования и вывода средств. Это может включать в себя скрытые комиссии, высокие пороги для вывода средств или даже отсутствие возможности вывода вложенных денег вовсе.

3. Использование лживой информации и фальшивых отзывов: Для привлечения новых клиентов мошеннические биржи часто создают ложные отзывы, поддельные рекомендации и искаженные данные

о своей деятельности. Это создает иллюзию успешной и надежной компании, призванной убедить инвесторов вложить свои деньги.

Для примера можно рассмотреть следующие мошеннические виды мошеннических проектов:

1. **Пирамиды.**

Пирамидные схемы являются одними из самых распространенных форм финансового мошенничества. Они предлагают инвесторам «легкую» прибыль за счет привлечения новых участников. Основная идея заключается в том, что старшие участники выигрывают за счет взносов новичков. Такие схемы неустойчивы и, когда приток новых участников замедляется, они обречены на крах, оставляя большинство участников без вложенных средств.

2. **Фейковые криптопроекты**.

В связи с возросшим интересом к криптовалютам, мошенники также начали использовать криптопространство для своих незаконных целей. Они предлагают ложные криптовалютные проекты с обещаниями быстрой и легкой прибыли. Однако за ними стоят скрытые мотивы и планы, которые могут привести к убыткам для инвесторов. **К примеру таких проектов, можно привести пример «https://tradestrike.net/», с помощью которого мошенники ввели в заблуждение жителя г. Молодечено и завладели 160009 белорусскими рублями**.

3. Звонки мошенников в месенджерах (Viber, Telegram, WhatsApp) под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, вынуждающих потерпевших под различными предлогами получать кредиты и переводить денежные средства либо сбережения на подконтрольные злоумышленниками счета – 517, или 46 %.

В текущем году наиболее актуальная схема – побуждение открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, поэтому для деактивации таких действий необходимо самостоятельно обратиться в банк и открыть кредит, и в дальнейшем перевести денежные средства на сберегательные счета. Как правило после перевода денежных средств связь с злоумышленников прекращается.

Наряду с этим в отчетном периоде зарегистрировано: **54** вымогательства (ст. 208 УК), **10** заведомо ложных сообщений об опасности (ст. 340 УК), **70** фактов незаконного оборота средств платежа и (или) инструментов (ст. 222 УК), **621** хищение имущества путем модификации компьютерной информации (ст. 212 УК) и **76** преступлений против компьютерной безопасности (глава 31 УК).

Основными способами совершения хищений имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса), являются:

1. Также звонки мошенников в мессенджерах под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, в ходе которых злоумышленники получают доступ к банковским реквизитам граждан (56,4 %).

Такой способ называется «Вишинг» – это один из методов мошенничества с использованием социальной инженерии (социальная инженерия – это совокупность способов психологического воздействия на поведение человека с целью получения выгоды), который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий
со своей банковской платежной картой

Он заключается в том, что злоумышленники, используя телефонную связь и, выдавая себя за сотрудников банка или правоохранительных органов, под различными предлогами вводят в заблуждение потерпевших, выясняя сведения о наличии банковских платежных карточках, их реквизитах, паспортных данных с целью последующего хищения денежных средств.

В большинстве случаев при совершении звонков мошенники используют интернет-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи.

При этом всем известные мессенджеры Viber, Telegram и WhatsApp имеют возможность использования виртуальных номеров.

К примеру, злоумышленники звонят жертве от имени банковского работника и сообщают, что необходимо осуществить какие-либо действия с банковской платежной карточкой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо проводит подозрительную оплату.

Для большей достоверности в качестве имени пользователя они указывают официальный номер банка либо его название, а для «аватарки» используют логотип или эмблему банковского учреждения.

При этом зачастую они уже владеют минимальной информацией о лицах, которым звонят (имя, отчество, дата рождения, последние цифры банковской карты и др.), что способствует повышению доверия к звонящему и производит на него определенное впечатление.

В дальнейшем преступник просит сообщить информацию о банковской карте – номер, срок действия, трехзначный код на ее обороте, содержание СМС-сообщения, которое в ходе разговора поступает
на мобильный телефон, либо устанавливает мобильное приложение, позволяющее злоумышленнику получить удаленный доступ к мобильному телефону, в котором сегодня фактически у каждого имеется интернет-банкинг и, соответственно, доступ к банковскому счету.

2. Использование фишинговых Интернет-ресурсов (25,4 %).

Фишинг – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет-ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (например, поддельные страницы услуги «Интернет-банкинг» различных банков).

К примеру в прошлом году житель нашей области, при попытке совершить платёж за коммунальные услуги посредством системы Интернет-банкинга, воспользовался поисковой строкой сайта Google и перешёл, как оказалось, по ложной ссылке для оплаты. Злоумышленникам стали известны реквизиты банковской карты и в результате с его карт-счета было похищено почти 35 тысяч рублей.

Также в социальных сетях появилась реклама, обещающая «призы от Белагропромбанка». Переходя по ссылке, жертва попадает на поддельную банковскую страницу, на которой мошенники выманивают номера телефонов и иные личные данные, что дает им полный доступ к счетам обманутых и даже возможность оформления онлайн-кредитов.

Распространены кибермошенничества от имени «Белпочты».

Схема довольно проста – злоумышленники присылают потенциальной жертве сообщение через интернет-мессенджер. В нем сообщают о необходимости уточнения адреса доставки почтового отправления и предлагают перейти по ссылке в Интернете. Невнимательный человек, не проверив адрес, по которому ему предлагают перейти, попадает на фейковый сайт, стилизованный под официальный сайт «Белпочты». Там клиента просят ввести свой адрес, якобы для доставки некоего почтового отправления, и оплатить тариф за услугу «Белпочты» прямо на этой странице, введя реквизиты банковской карты.

Появились случаи мошенничеств, связанных с созданием фейкового аккаунта в мессенджерах от имени руководителя учреждения, где работает потенциальная жертва.

Злоумышленники осуществляют рассылку сообщений с указанием того, что в скором времени гражданину позвонит или напишет сотрудник

вышестоящей инстанции (Министерства образования, МВД, КГБ, КГК, СК, ОВД). Как правило, пугаясь, граждане говорят любую информацию, которую требует сотрудник. Далее просят установить удаленное программное обеспечение, позволяющее получить ему доступ к устройству, либо вести видеозапись с демонстрацией экрана мобильного телефона.

Преступления против компьютерной безопасности в большинстве случаев возбуждаются по фактам неправомерного завладения учетными записями мессенджеров и социальных сетей, таких как **(Telegram (34), WhatsApp (3), Instagram (7), Facebook (1) и «ВКонтакте» (13)**.

Основные способы совершения вымогательств (ст. 208 Уголовного кодекса), можно разделить на три основные категории:

1) связаны с **угрозой распространения личной информации потерпевших, которые последние желали сохранить в тайне** (27, или 50 %), как правило фотографий и видеозаписей интимного характера, которые, в большинстве случаев, потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером противоположного пола для знакомства.

2) связаны с **блокированием компьютерной информации** физических лиц (24 или 44,4 %). При этом в подавляющем большинстве случаев отмечается блокирование учетных записей Apple ID посредством ввода авторизационных данных, предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.

3) связаны с **угрозой применения насилия** (3 или 5,6 %).

Стоит отметить, что **81 %** всех совершенных заведомо ложных сообщений об опасности по линии ПК, составляют **«сватерскую»** направленность, то есть отправку заведомо ложного сообщения об опасности от лица жертвы, посредством электронной почты.

Основными факторами, способствующими совершению киберпреступлений, являются халатность, излишняя доверчивость граждан, мнимая возможность быстрого обогащения, получение крупных сумм денежных средств, а также недостаточное информирование населения о способах и методах применяемыми преступниками при совершении указанных преступлений.

Знание основных схем и способов обмана позволяет гражданам быть более внимательным и осторожным, что, в свою очередь, помогает предотвратить случаи совершения киберпреступлений.

Экспоненциально увеличивающийся поток информации и преобладание цифровой информации в образовательной среде

современной школы актуализируют проблему профилактики цифровой безопасности современных школьников. Особое место в данном вопросе принадлежит профилактике цифровой зависимости школьников, поскольку дети проводят в интернете довольно много времени.

Как известно, интернет не только содержит множество полезной информации и предоставляет выбор развлечений, но и таит массу угроз, которые могут повлиять и на материальное состояние семьи, и на психологическое здоровье детей.

На текущий момент возраст интернет-пользователя снизился настолько, что порой пятилетние малыши обращаются с компьютером и мобильными устройствами более ловко, чем взрослые. Помимо всех известных положительных моментов, интернет несет в себе опасность, которая может затронуть даже пользователей младшего дошкольного возраста.

СОВЕТЫ ПО БЕЗОПАСНОСТИ

Существенную часть своей жизни современные дети и подростки проводят в интернете, а значит без базовых знаний в области кибербезопасности им, как и взрослым, не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

Советоваться с родителями

Если ребенок хочет зарегистрироваться на каком-либо сайте, создать профиль в социальной сети и выложить свои фотографии, лучше перед этим посоветоваться с родителями. Взрослый человек сможет лучше проанализировать ситуацию и понять, опасен ли сайт, а также помочь выбрать снимки, которые можно выложить на всеобщее обозрение.

Установить дистанционный контроль

Функция **«родительского контроля»** – это и как специализированное ПО, так и услуги провайдера, которые включает в себя стандартный набор функций. А именно:

- ограничение времени нахождения ребенка в сети;
- ограничение времени пользования компьютером;
- возможность создания графика с допустимыми часами работы в течение дня;
- блокировка сайтов с запрещенным контентом;
- ограничение на запуск приложений (например, игр и иных приложений) и установку новых программ;

Беречь личные данные

Даже если ребенок думает, что хорошо знает человека, с которым общается онлайн, не нужно рассказывать подробности о себе и о родителях. Номер телефона, адрес, номер школы и класса, место работы родителей и их график, время, когда в квартире нет взрослых, а также данные из документов, номера банковских карт – такую информацию ни в коем случае нельзя передавать другим людям.

Не делиться информацией о знакомых

Правило, приведенное выше, распространяется и на других людей. Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают. Нельзя показывать их фотографии – ни выкладывать их в своих профилях в социальных сетях, ни тем более в частной переписке.

Если хочется выложить групповое фото с праздника или тренировки, сначала стоит обсудить это с теми, кто изображен на снимке. И лучше, если они сообщат родителям, что такое фото публикуется в интернете.

Фильтровать информацию

Мошенники активно используют интернет в своих интересах. Они могут обманывать людей и манипулировать ими, давя на жалость или страх. Поэтому надо научиться скептически относиться к любой информации, размещенной в интернете, и не доверять слепо всему, что там пишут.

Слуцкий район

На территории Слуцкого района количество регистрируемых преступлений по линии противодействия киберпреступности на октябрь 2024 увеличилось в сравнении с аналогичным периодом прошлого года с 80 до 124, или рост +55 %. Зарегистрировано 16 преступлений, относящихся к категории тяжких и особо тяжких (АППГ – 8) из которых 9 преступлений остаются нераскрытыми (не установлено лицо его совершившее).

Справочно: К категории тяжких и особо тяжких преступлений в основном относятся те, по которым злоумышленники завладели денежными средствами в сумме свыше 250 базовых величин (10000 рублей НБ Республики Беларусь).

Структура преступности по линии противодействия киберпрестпуности сложилась следующим образом:

1) хищения имущества путём модификации компьютерной информации (ст.212 УК Республики Беларусь)

33 от общего количества совершенный преступлений или 26,61 %

2) мошенничество (ст. 209 УК Республики Беларусь)

57 от общего количества совершенный преступлений или 45,97 %

3) несанкционированный доступ к компьютерной информации (ст. 349 УК Республики Беларусь)

6 от общего количества совершенный преступлений или 4,83 %

4) вымогательство (ст. 208 УК Республики Беларусь)

1 от общего количества совершенный преступлений или 0,8 %

5) преступления в части предоставления банковских сведений (ст. 222 УК Республики Беларусь и т.д.)

27 от общего количества совершенных преступлений или 21,77 %;

Следует отметить тот факт, что значительный рост преступлений, предусмотренных ст. 209 УК Республики Беларусь выражен в том, что потерпевшие лица либо желали приобрести товар (как правило в социальной сети «Instagram») по необоснованно низкой цене, либо под предлогом заработка денежных средств осуществляли денежные переводы на так называемые «биржи».

Проблематика приобретения вещей в социальной сети «Instagram» заключается в том, что злоумышленники щепетильно подходят к оформлению персональной страницы, что выражено в накрутке активности (лайки, комментарии, подписчики, отзывы о приобретении товара и т.д.), в т.ч. параллельно путем обмана склоняют 3-х лиц к открытию на свое имя как правило «ИП» и уже в дальнейшем таковые реквизиты указывают в шапке профиля, что значительно снижает бдительность граждан, при этом предварительно указывая данным лицам о необходимости предоставления мошенникам всей оформленной документации, что выступает в роли «гаранта» при совершении дальнейший противоправных действий. Также следует отметить, что реальные аккаунты, которые действительно осуществляют предпринимательскую деятельность, взламываются злоумышленниками, которые в дальнейшей продолжают мнимую деятельность, что фактически не предоставляет шансов потерпевшей стороне понять, что они могут быть обманутыми.

В данном случае, чтобы прибегнуть к стабильной тенденции снижения преступлений указанной категории, необходимо работать с населением и разъяснять, что факты предоплаты на неизвестные банковские счета нужно исключить и целесообразнее приобретать таковые вещи посредством почтового отправления оплачивая таковой товар при реальном получении.

Справочно. На территории обслуживания Слуцкого РОВД зафиксированы факты преступлений со стороны следующих персональных аккаунтов «airmac_by» (продажа моб. устройств марки Iphone), «buketbel.by» (продажа цветов), «mirelor_by» (продажа новогодних украшений), «esya_step_by» (продажа молодежной одежды), «hochukreslo.by» (продажа различного рода предметов интерьера) и т.д.

Неустановленное лицо в период времени с сентября 2023 года по январь 2024 года гражданин г. Слуцка общаясь посредством различного рода мессенджеров сети Интернет с представителями брокерской компании желая заработать денежные средства осуществил денежные перевод в общей сумме не менее 38100 рублей НБ Республики Беларусь, которые в дальнейшем выступали в роли ставок на торгах связанной с нефтью, золотом и криптовалютой и т.д.

Помимо указанного имеют место единичные факты совершения противоправных действий **посредством «вишинга».** Это метод мошенничества заключается в том, что злоумышленники, используя телефонную коммуникацию, звоня потерпевшей стороне и играя определенную роль (сотрудника банковской сферы, правоохранительных органов, операторов сотовой связи и т.д.) под разными предлогами выманивают у граждан конфиденциальную информацию, в т.ч. склоняют к осуществления денежного перевода. Как практика показывает все телефонные звонки начинаются с того, что потерпевшей стороне указывают о том, что на их имя происходило оформление кредита, оформление сим-карт, с их банковских счетов осуществляется финансирование СВО в Украине и все эти действия связаны с совершением преступлений, что вызывает у таковых «сотрудников» необходимость в проведении обыска и т.д. Все это вызывает у людей острую необходимость в решении данной проблемы, в следствие чего люди выполняют все те действия, которые озвучивают им мошенники (осуществление денежного перевода на сберегательные счета, оформление кредитного договора для вычисления злоумышленников в банковской сфере, в т.ч. при отсутствии денежных средств склоняют к продаже своего личного имущества, сдачи такового имущества в ломбард под залог, а в следствие и к дальнейшему денежному перевода на сберегательные счета.)

Справочно: Зачастую таковые телефонные звонки при «вишинге» осуществляются посредством звонков в мобильных приложениях «Viber», «Telegram», «WhatsApp», при этом таковые звонки и поступают посредством мобильном связи.

Неустановленное лицо, в период времени с 07.10.2024 по 19.10.2024, в ходе осуществления телефонных звонков, в т.ч. мессенджерах, с

гражданкой г. Слуцка, представившись сотрудниками правоохранительных органов, убедивши последнюю об утечке персональных данных последней и использовании их в противоправной деятельности, под предлогом выявления недобросовестных работников банковских учреждений, убедили последнюю получить кредиты в ЗАО "МТБанк", ОАО "Сбер Банк" и ЗАО "АльфаБанк" на общую сумму 68000 рублей НБ РБ, после чего убедило перечислить указанные денежные средства, а также личные сбережения в сумме 6760 рублей, на предоставленные неизвестным лицом банковские счета, тем самым похитив денежные средства в общей сумме ***не менее 74700 рублей.***

Неустановленной лицо в мессенджере «WhatsApp» связались с гражданином г. Слуцка представившись сотрудников УП "А1" указали о необходимости сообщения всех приходящих кодов доступа, в т.ч. установлении приложений на свое мобильное устройство, после чего произошло списание денежных средств не менее 10980 рублей НБ Республики Беларусь.

Также следует отметить, что вплоть до настоящего момента актуальна форма совершения противоправных действий **как «фишинг».** Указанная форма противоправных действий заключается в том, что злоумышленники создают копии различных Интернет-ресурсов (как правило банковских учреждений, но в т.ч. почтовых организаций Европочта, Сдэк), где потерпевшая сторона указывает свои банковские сведения (номер банковской платежной карты, CVV код, в т.ч. иную личную информацию) в следствие чего происходило списание денежных средств

Отличить «фишинговый ресурс» можно только по электронному адресу и как практика показывает таковые заканчивают на раздичные варианты доменов «.ru», «.com», «.site», «.online» и т.д., при этом практически все официальные ресурсы Республики Беларусь заканчиваются на домен «.by».

Справочно. 12.03.2024 гражданин г.Слуцка используя персональный мобильный гаджет, осуществила вход на фишинговый интернет-ресурс "ОАО "АСБ Беларусбанк" «ibank.belarussbank.com» где осуществила ввод данных банковской платежной карты ОАО "АСБ Беларусбанк», после чего произошло списание денежных средств в сумме 395 рублей НБ Республики Беларусь.

Помимо указанного проблемным вопросом на территории Слуцкого района является тот факт, что на настоящее время возбуждено 27 уголовных дел по ст. 222 УК РБ (передача реквизитов банковских карт) Фигурантами уголовных дел стали студенты учреждений образования Слуцкого района.

Во всех зафиксированных случаях подозреваемые действовали по одной схеме. По просьбе друзей или знакомых за вознаграждение от 5 до 100 рублей открывали на свое имя личные кабинеты в «М-Банкинге» разных банков Беларуси. Все это делалось дистанционно со своих мобильных телефонов. Процедура оформления таковых кабинетов максимально проста, для этого необходимо ввод в приложении своего идентификационного номера и приходящих кодов-доступа на абонентский номер. Оформление занимает около 5 минут. После того, как случчане оформляли личные кабинеты, за материальное вознаграждение они передавали логин и пароль доступа от М-Банкинга мошенникам, которые уже в дальнейшем использовали таковые банковские счета в своих преступных целях.

Следует отметить, что один инициативный студент, найдя объявление в интернете о подобном «заработке», может втянуть в преступную схему значительное количество добропорядочных ребят. Которые, не зная всей ответственности и последствий, по просьбе знакомого или друга откроют такие счета, не придав этому абсолютно никакого значения.

В нынешних реалиях, чтобы не стать жертвой кибермошенников, стоит неукоснительно соблюдать следующие правила:

- никогда не сообщайте незнакомым лицам, в т.ч. в ходе телефонных разговора свои персональные данные, реквизиты своих БПК в т.ч. доступа к мобильному банкингу;
- не переходить по неизвестным ссылкам, которые Вам присылают в сети Интернет, особенно где просят указать свои банковские карты;
- в случае утери или кражи карты заблокируйте ее по телефону или в банке;
- исключите осуществление предоплаты при приобретении товаров или услуг в сети «Интернет».

Материал подготовлен отделом внутренних дел Слуцкого райисполкома