Вопросы информационной и кибербезопасности

В Республике Беларусь отмечается рост преступлений, совершаемых с использованием информационно-коммуникационных технологий в отношении работников различного рода учреждений и предприятий.

Жертвами преступников в 2024 г. стали 4 представителя УО «ГрГМУ», которые лишились значительных денежных сумм.

11-12 ноября 2024 г. посредством мессенджера Telegram в адрес более 30 представителей нашего университета поступили направленные мошенниками сообщения. При этом использовалась схема «Fake boss» *(описание в последующих слайдах).*

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

МОШЕННИК МОЖЕТ ПРЕДСТАВИТЬСЯ:

- сотрудником банка
- сотрудником правоохранительных органов
- родственником или другом из социальных сетей

И НАЗВАТЬ ПРИЧИНУ ЗВОНКА:

- вам одобрен кредит
- по вашему счету обнаружены мошеннические операции
- подтверждение оформления доверенности на операции по вкладу

МОШЕННИК МОЖЕТ ПОПРОСИТЬ:

- назвать номер, срок действия и трехзначный код на обороте карты, коды из смс-сообщений
- войти в ваш интернет-банкинг и проверить не изменился ли баланс счета
- назвать или напечатать цифры из смс-сообщения
- установить программу или мобильное приложение для отмены операции по счету или защиты своего счета от мошенников
- помочь разоблачить недобросовестного сотрудника банка
- оформить кредит в банке
- перевести деньги на «защищенный» счет

Представители банков и правоохранительных органов Республики Беларусь не пользуются интернет-мессенджерами для работы с гражданами.

Именно телефонные мошенники в подавляющем большинстве случаев для связи с потенциальной жертвой используют различные мессенджеры (*Viber, Telegram, WhatsApp*).

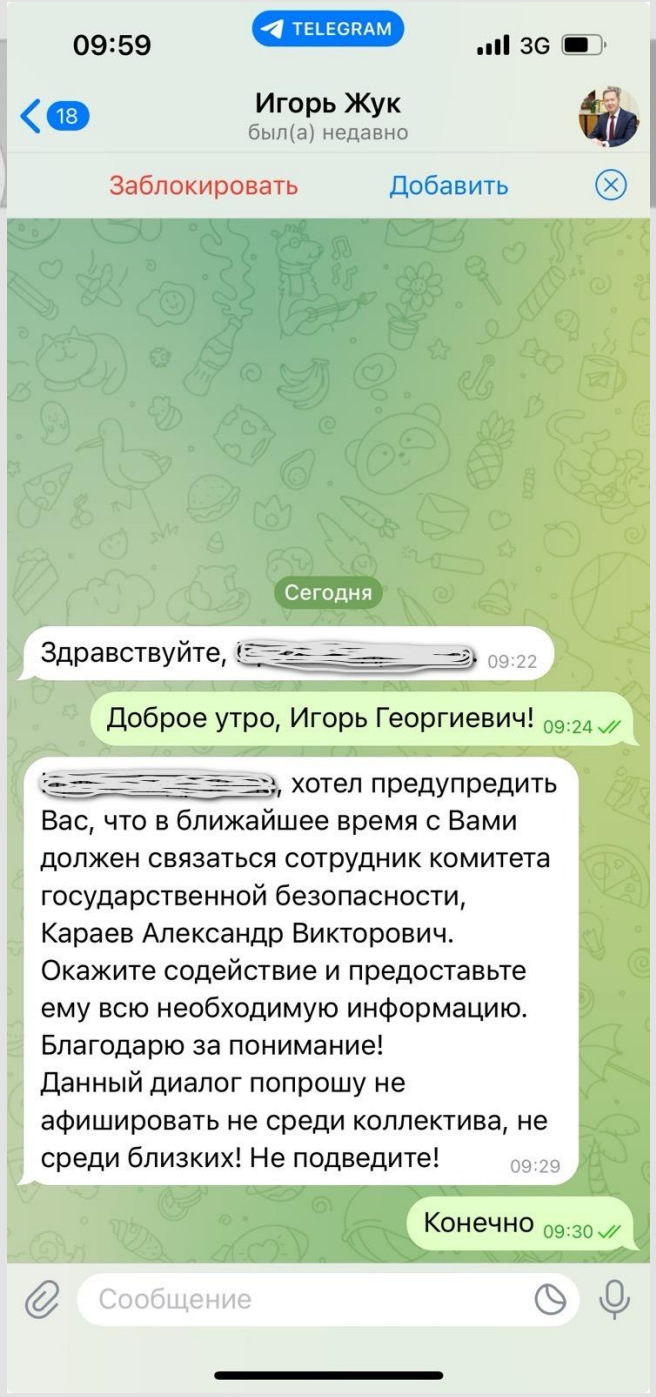
Не вступайте в контакт и не ведите разговоры со лжеправоохранителями, не выполняйте их инструкции!

Прекратите разговор, заявив, что будете общаться лишь в официальном офисе правоохранительного органа при вызове туда соответствующей повесткой.

Мошенничество по схеме Fake boss

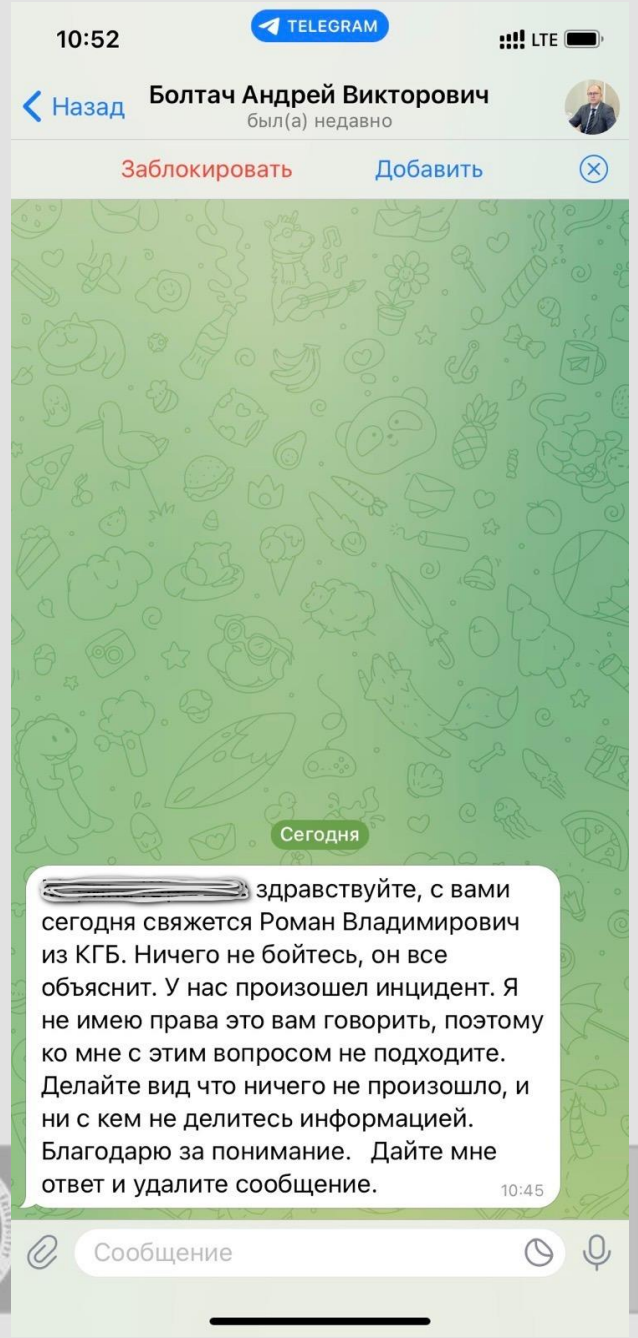
Для реализации такой схемы **преступники изучают чаты трудовых коллективов в мессенджерах, собирают информацию об организации и руководителях, создают учетные записи от их имени**. С помощью фейкового аккаунта руководителя они вступают в переписку с подчиненными и, используя доверие к начальнику, дают определенные указания или разъяснения. В частности, о необходимости контакта с конкретным «представителем правоохранительных органов».

Указанный психологический прием в ряде случаев снижает уровень критической оценки гражданином последующих действий преступников, обеспечивая беспрекословное выполнение поступающих от них указаний.



Мошенничество по схеме Fake boss

Далее гражданину поступают звонки посредством мессенджеров от «сотрудников правоохранительных органов», в некоторых случаях с демонстрацией фотографий поддельных служебных удостоверений.



Мошенничество по схеме Fake boss

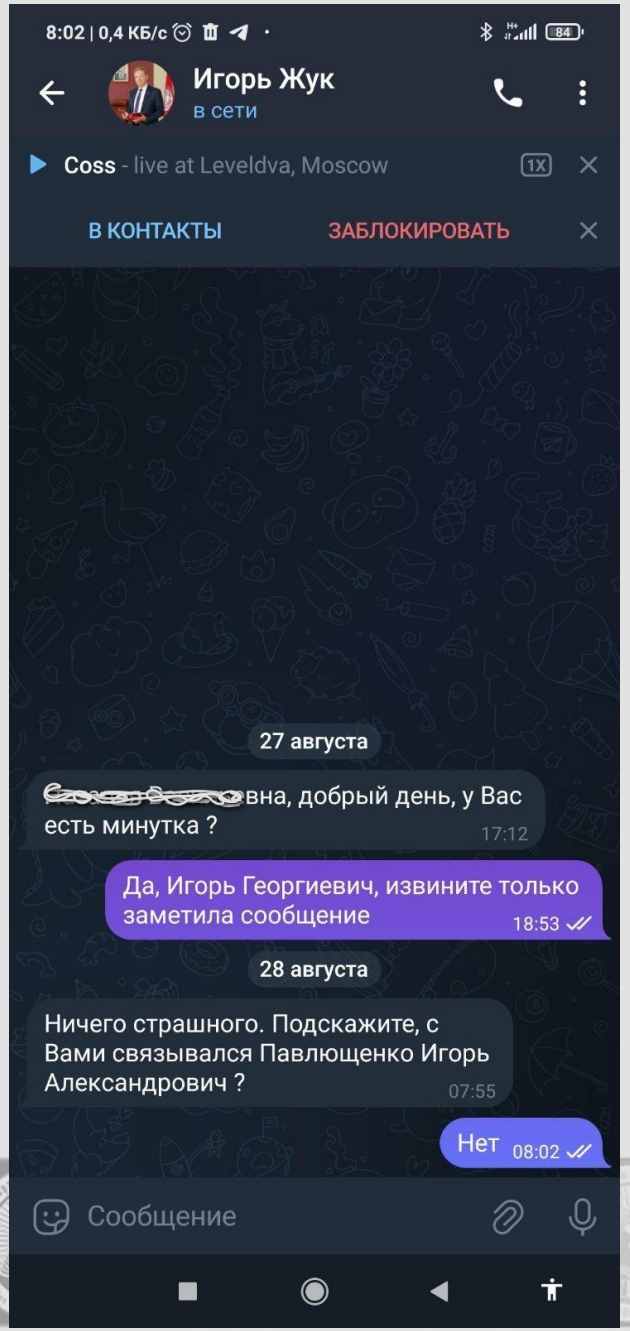
В ходе беседы псевдосотрудники убеждают в необходимости совершения определенных действий, в том числе по перечислению денежных средств под различными мошенническими предлогами:

- участие в специальной операции по поимке «преступников», которые якобы пытаются похитить деньги с использованием счетов гражданина или от его имени;
- наличие информации о якобы совершении гражданином преступных финансовых операций, для снятия подозрения, в которых необходимо совершить требуемые действия;
- планируемое проведение обыска по месту жительства гражданина с целью выявления и изъятия незадекларированных наличных денежных средств.

Мошенничество по схеме Fake boss

Убедив жертву в правомочности своих действий, звонящий предлагает:
- передать посреднику наличные денежные средства или внести их на указанные банковские счета;
- перечислить денежные средства с банковских счетов, в том числе оформив на свое имя для этих целей кредиты;
- предоставить реквизиты своих банковских карт, аутентификационные данные для доступа к банковским счетам, коды из поступивших sms-сообщений и т.д.

Наиболее часто указанная мошенническая схема используется среди работников сфер образования и здравоохранения.



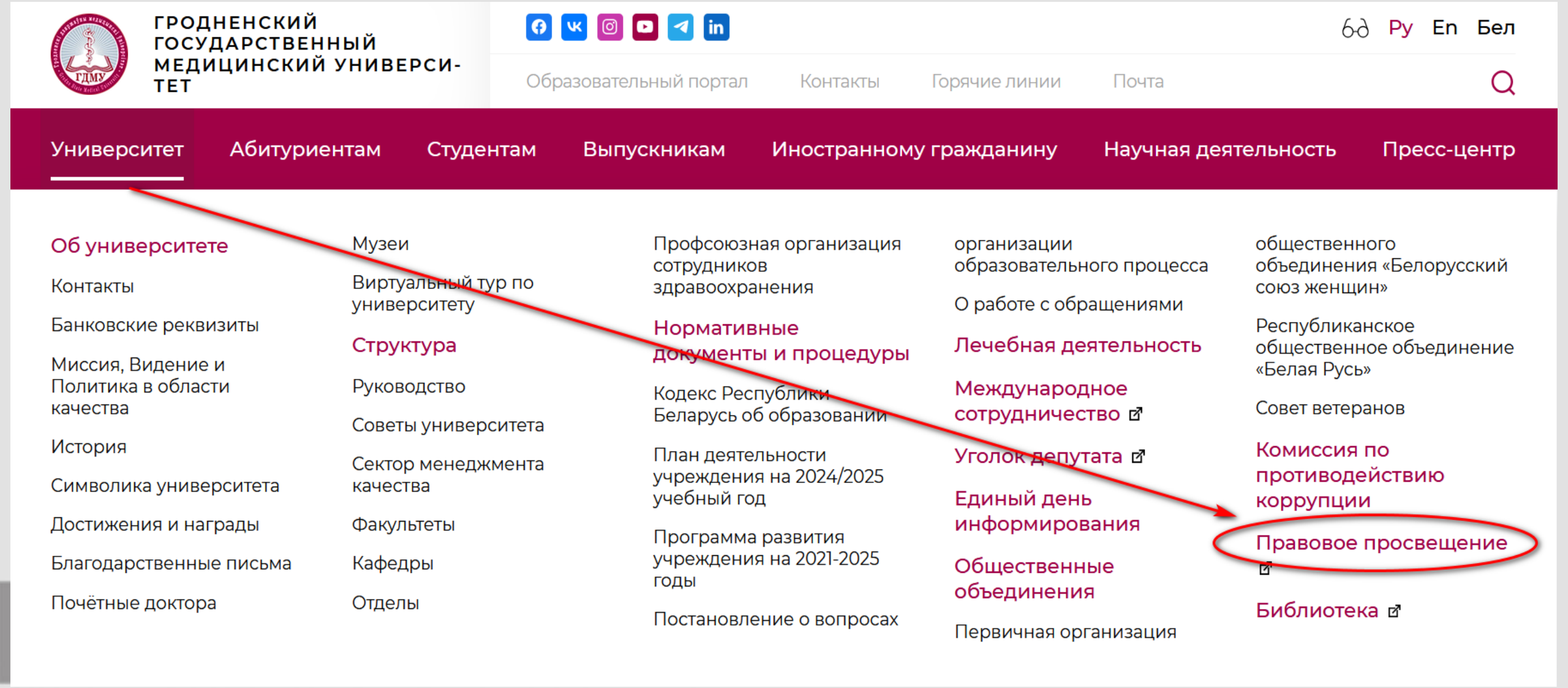
Мошенничество по схеме Fake boss

При поступлении подобных сообщений в мессенджерах могут быть рекомендованы следующие действия:

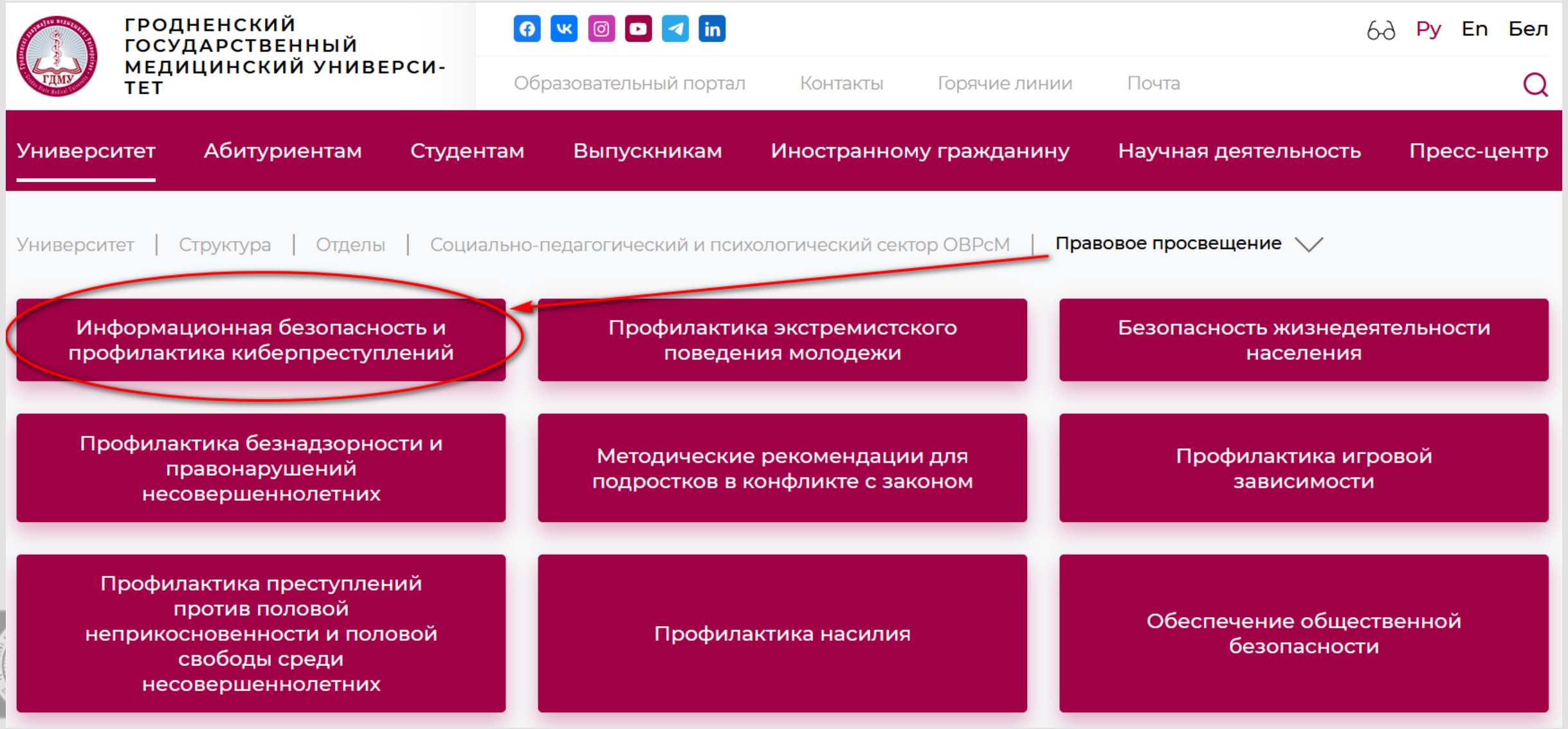
- Убедитесь в правильности названия аккаунта и номера телефона.
- Проверьте историю сообщений и убедитесь, что у вас есть контакт с коллегой (если Вы уже общались ранее, то вверху диалога не должно быть кнопок «В контакты» и «Заблокировать»).
- Если сомневаетесь в том, что вам пишет коллега, попросите его написать посредством иного мессенджера или позвонить на городской телефон.
- Свяжитесь с коллегой по городскому или мобильному телефону и уточните, направлялись ли им в Ваш адрес какие-либо сообщения.
- Не выполняйте никаких требований финансового характера, никому не сообщайте реквизиты банковских карт и т.д.

Будьте бдительны – мошенники на регулярной основе совершенствуют схемы обмана людей.

Предлагается ознакомиться с содержанием размещенных в тематической рубрике материалов и руководствоваться ими в повседневной жизни



Предлагается ознакомиться с содержанием размещенных в тематической рубрике материалов и руководствоваться ими в повседневной жизни



Профилактика киберпреступлений (памятки, информационные письма, конспекты)

Ответственность за регистрацию на интернет ресурсах, призванных экстремистскими, распространение экстремистских материалов в глобальной сети интернет

Ответственность за использование беспилотных летательных аппаратов (квадрокоптеров)

О профилактике преступлений против собственности и информационной безопасности

Информационное письмо о состоянии преступности, связанной с неправомерным завладением реквизитми пластиковых банковских карт

Профилактика наиболее распространенных видов преступлений против информационной безопасности

Профилактика хищений денежных средств граждан с использованием информационно-коммуникационных технологий

Предупреждение мошенничеств, в т.ч. совершаемых с использованием компьютерной техники

Возможные схемы работы мошенника

Как не стать жертвой киберпреступника

О профилактике преступлений против собственности и информационной безопасности

Информационное письмо о состоянии преступности, связанной с неправомерным завладением реквизитми пластиковых банковских карт

Профилактика наиболее распространенных видов преступлений против информационной безопасности

Профилактика хищений денежных средств граждан с использованием информационно-коммуникационных технологий

Предупреждение мошенничеств, в т.ч. совершаемых с использованием компьютерной техники

Возможные схемы работы мошенника

Как не стать жертвой киберпреступника

Профилактика киберпреступлений

Памятка об актуальных способах совершения преступлений в Интернете

Интернет-мошенничество

ЗАЩИТА БАНКОВСКОЙ КАРТОЧКИ

Основные правила информационной безопасности по защите банковской карточки:

- хранить в тайне пин-код карты
- прикрывать ладонью клавиатуру при вводе пин-кода
- оформлять отдельную карту для онлайн-покупок
- деньги зачислять только в размере предполагаемой покупки
- использовать услугу 3-D Secure* и лимиты на максимальные суммы онлайн-операций
- скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его
- подключить услугу "SMS-оповещение"

Не рекомендуется

- хранить пин-код вместе с карточкой/на карточке
- сообщать CVV-код или отправлять его фото
- распространять личные данные (например паспортные), логин и пароль доступа к системе "Интернет-банкинг"
- сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли***, код авторизации, пароли 3-D Secure

Руководителям структурных подразделений предлагается:

- активизировать проводимую в коллективах профилактическую и информационно-разъяснительную работу, направленную на повышение цифровой грамотности работников, осознания ими необходимости соблюдения основных правил кибербезопасности и недопущения беспечного поведения.