ный розыск «Оповещение» в подсистеме ИБД-Ф). Создание такой вкладки позволит УУП оперативно проверять на законных основаниях граждан на предмет их нахождения в розыске, в том числе по преступлениям прошлых лет.

УДК 378

***М.Г. Гизатуллин***

## НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Рассматривая направление обеспечения национальной безопасности того или иного государства, нельзя не отметить, что вопросы, относящиеся к организации и реализации образовательной деятельности, с позиции различных уровней образования, так же, как и другие вопросы данного направления, являются одним из ключевых направлений развития и функционирования государства в целом, определяют вектор его стратегического развития. Иными словами, образование выступает своего рода приоритетным направлением развития любого современного государства. Изучая же вопросы организации и реализации образовательного процесса в той или иной образовательной организации, например, высшего образования того или иного государства, необходимо отметить, что образовательный процесс в данном случае представляет собой непрерывный процесс становления обучающегося (студент, курсант, иностранный обучающийся), как личности, индивида, «профессионала» в той или иной области (сфере) деятельности. Этот процесс направлен на формирование у обучающегося знаний, умений, навыков и (или) опыта деятельности по определенному направлению подготовки (специальности), которые реализуются в той или иной образовательной организации.

Образовательные организации высшего образования России и государств – участников Международной парламентской ассамблеи (МПА) СНГ различных министерств и ведомств имеют как сходные, так и разные признаки, которые присущи различным видам деятельности, реализующимся в образовательных организациях.

В 2021 г. Министр внутренних дел Российской Федерации В.А. Колокольцев официально заявил: «Основное влияние на рост тяжких преступлений по итогам 2020 года оказало увеличение количества крими-



нальных деяний данной категории, совершенных с использованием информационно-телекоммуникационных технологий». Были и другие официальные заявления. Возможно, озвучивание данных проблем на государственном уровне и повлияло на то, что в 2021 г. почти все образовательные организации высшего образования системы МВД России перешли на так называемый новый формат с позиции, например, основных профессиональных образовательных программ высшего образования по специальностям и направлениям подготовки. Этот «новый формат» является актуальным направлением не только с позиции «теоретиков», но и с позиции «практиков». Иными словами, данное направление затрагивает как обучающихся образовательных организаций высшего образования системы МВД России, так и сотрудников территориальных органов МВД России. Это направление прежде всего касается формирования у обучающихся образовательных организаций высшего образования системы МВД России ключевых знаний, умений, навыков и (или) опыта деятельности в рамках такого достаточно актуального и востребованного в наши дни направления (в том числе в условиях нестабильной геополитической ситуации в мире), как организация кибербезопасности и обеспечение противодействия киберпреступности.

Сегодня многие организации, предприятия, учреждения той или иной области (сферы) деятельности испытывают на себе достаточно агрессивное, негативное, деструктивное и т. д. проявление со стороны определенного типа лиц – злоумышленников. Они подвержены, например, различного рода и типа кибератакам как извне, так и, к сожалению, в ряде случаев – изнутри, с целью осуществления своего рода дестабилизации как самой организации, учреждения, предприятия, так и государства в целом.

Таким образом, в 2021 г. в образовательных организациях системы МВД России почти по всем специальностям и направлениям подготовки появилась новая учебная дисциплина «Основы кибербезопасности». Ранее же вопросы обеспечения безопасности информации и противодействия различного рода и типа угрозам изучались обучающимися на таких учебных дисциплинах, как «Информатика и информационные технологии в профессиональной деятельности», «Основы информационной безопасности в органах внутренних дел» и др.

Учебная дисциплина «Основы кибербезопасности», реализуемая с 2021 г. в Уральском юридическом институте МВД России (далее – УрЮИ МВД России), прежде всего ориентирована на изучение обучающимися:

нормативно-правового регулирования в области информационных технологий, в том числе в области обеспечения кибербезопасности как на уровне государства, так и на уровне деятельности органов внутренних дел;

способов, методов, приемов и средств в области организации и реализации обеспечения безопасности различных вычислительных устройств;

природы возникновения и реализации различных каналов утечки информации;

вопросов в области организации и реализации обеспечения технической защиты информации, а также криптографической и стеганографической защиты информации;

вопросов в области различных инцидентов, возникающих на базе имеющегося у «пользователя» аппаратного обеспечения, программного обеспечения, информационных ресурсов, среды передачи, а также правил и алгоритмов реагирования на них и их детальную обработку и др.

УрЮИ МВД России на базе имеющихся компьютерных классов, полигонов, центров и других объектов также осуществляет проведение киберучений для закрепления у обучающихся компетенций, приобретаемых ими на учебных занятиях и в ходе самостоятельного изучения разделов учебной дисциплины «Основы кибербезопасности» в рамках внеаудиторной самостоятельной работы.

После завершения 2021/2022 учебного года и начала 2022/2023 учебного года в УрЮИ МВД России, помимо достаточно большого количества положительных моментов от появления в учебных планах учебной дисциплины «Основы кибербезопасности», можно выделить ряд потребностей субъектов образовательного процесса в рамках совершенствования методики проведения учебных занятий.

При этом достаточно важным направлением в области организации и реализации образовательного процесса является рассмотрение вопроса о необходимости оснащения автоматизированных рабочих учебных мест обучающихся (с позиции практической реализации):

системами, основанными на реализации сбора и анализа информации о тех или иных событиях, появляющихся на базе имеющихся у «специалиста» аппаратного обеспечения, программного обеспечения, информационных ресурсов и среды передачи (SIEM);

системами, основанными на реализации фильтрации трафика организации, учреждения, предприятия, а также его анализа (DLP).

Полагается, что учебная дисциплина «Основы кибербезопасности» может также найти свое отражение и в образовательных организациях системы МВД государств – участников МПА СНГ для формирования у обучающихся данных организаций компетенций в области организации кибербезопасности и обеспечения противодействия киберпреступности.



УДК 343.79

***М.Г. Головенчик***

## КИБЕРПРЕСТУПНОСТЬ И ЭКОНОМИЧЕСКАЯ ПРЕСТУПНОСТЬ: ПРОБЛЕМЫ СООТНОШЕНИЯ

В соответствии с Концепцией информационной безопасности Республики Беларусь под киберпреступлениями понимаются предусмотренные Уголовным кодексом Республики Беларусь (далее – УК Беларуси) преступления против информационной безопасности. В УК Беларуси данным преступлениям посвящен разд. XII, гл. 31, где рассматриваемые преступления называются преступлениями против компьютерной безопасности. К таким преступлениям, в частности, относится несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации) (ст. 349 УК Беларуси), умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этим системе или сети, повлекшее по неосторожности причинение существенного вреда (ст. 355 УК Беларуси) и др.

Вместе с тем противодействие киберпреступности, в том числе подготовка специалистов в данной сфере, должно учитывать и то, как киберпреступления соотносятся с иными преступлениями, связанными с цифровой информационной средой.

Рассмотрим эту проблематику на примере экономических преступлений, к которым относят преступления, указанные в гл. 25 «Преступления против порядка осуществления экономической деятельности» УК Беларуси. В условиях цифровизации такие преступления также могут совершаться с помощью информационно-коммуникационных технологий, способами, сходными со способами совершения киберпреступлений. В этой связи может быть затруднительно отграничивать их друг от друга в практической деятельности. Так, в частности, ст. 222 УК Беларуси запрещает изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам. Последующее получение доступа к счетам или электронным кошелькам ставит вопрос о том, что в данном случае совершено: экономическое преступление или киберпреступление?