Шинкарев Александр Александрович,
курсант учебной группы 20об6г
факультета подготовки специалистов ГИБДД
ОрЮИ МВД России им. В.В. Лукьянова, г. Орёл

Научный руководитель:
Смирнов Иван Михайлович,
кандидат исторических наук,
старший преподаватель кафедры ОРД ОВД
ОрЮИ МВД России им. В.В. Лукьянова, г. Орёл

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
METHODS OF COUNTERING CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Аннотация: В статье рассматриваются проблемные аспекты проведения всестороннего и комплексного анализа противодействия преступлениям в сфере информационных технологий, а также выявление наиболее актуальных проблем в рассматриваемой области и поиск возможных путей решения данных проблем.

Abstract: The article discusses the problematic aspects of conducting a comprehensive and comprehensive analysis of countering crimes in the field of information technology, as well as identifying the most pressing problems in the field under consideration and finding possible solutions to these problems.

Ключевые слова: Информационные технологии, угрозы, информационные системы, безопасность.

Keywords: Information technologies, threats, information systems, security.

В настоящее время для противодействия преступности в сфере информационных технологий требует неотложного совершенствования и развития действующей системы борьбы с киберпреступностью как целостной, интегрированной структуры, объединяющей противодействие киберпреступности на всех направлениях, включая и новое его проявление. Назовём некоторые способы борьбы с киберпреступниками:

1) Одним из инструментов противодействия кибермошенничеству является уголовно-правовой институт как в рамках национального законодательства, так и на уровне международном. В условиях борьбы с преступностью в интернет-сфере особую значимость приобретает предупредительная функция уголовно-правовой системы.

2) Другим эффективным путем самозащиты личной информации является правильное использование надежного антивирусного ПО.

3) Следующим механизмом борьбы с кибермошенниками можно назвать правоохранительные органы, которые если обнаруживают сайты с террористической или экстремистской информацией, то они связываются с провайдером, предупреждают его и просят принять меры, ограничивающие доступ к подобной информации. [1]

Таким образом, термин «кибербезопасность» можно использовать, если четко определить границы правового регулирования, государственного вмешательства в регулирование общественных отношений, связанных с цифровой средой. Чрезмерное присутствие государства приводит к негативным последствиям, прежде всего – к стагнации, а не развитию экономики. В то же время необходимо активизировать участие государства в обеспечении кибербезопасности, в том числе в определении понятия и видов киберпреступности, мер борьбы с этим явлением, подготовке специалистов соответствующей квалификации.

Неправомерный доступ к информации, обрабатываемой в информационных системах, – это частое явление. Для предупреждения несанкционированного ее получения разрабатываются и внедряются системы защиты информации (СЗИ). Под СЗИ понимается совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.[2] Тем не менее, даже грамотно разработанная политика безопасности не может гарантировать безопасность информации, угроза ее утечки достаточно высока. Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

В жизненном цикле любой информационной системы является обязательным проведение мониторинга и анализа угроз, в соответствии с этим приведем общую их классификацию. Выделим признаки угроз:

– по природе происхождения;
– по характеру воздействия;
– по последствиям от их реализации;
– по способам реализации;
– по объектам воздействия.

По природе происхождения угрозы делятся на два класса: естественные и искусственные.

Естественные угрозы представляют собой воздействие на систему объективных процессов или явлений природы, в которых человек не принимает участия. Искусственные угрозы, соответственно, созданы человеком. Они в свою очередь подразделяются на угрозы по характеру воздействия: непреднамеренные и преднамеренные. Непреднамеренные вызваны различного

рода ошибками в проектировании, ошибками персонала и т.п. Преднамеренные характеризуются осознанными вредоносными действиями злоумышленника.

По характеру последствий от угроз, реализация которых приводит к нарушению конфиденциальности, целостности, доступности информации, как по отдельности, так и в различных комбинациях.

Угрозы по способам их реализации можно разделить на три вида:

– угрозы несанкционированного использования компьютерных ресурсов;

– угрозы, приводящие к появлению уязвимостей при сетевом взаимодействии;

– угрозы, допускающие физические способы нанесения ущерба. [3]

При рассмотрении выделяется множество объектов воздействия угроз информационной безопасности, как и их классификаций.

Таким образом, можно сделать вывод о том, что у злоумышленника очень много вариантов проведения атак на информационную систему. Тем самым создаются многочисленные проблемы для противоборствующей стороны.

Выделенные признаки угроз информационной безопасности составляют основу для предупреждения преступлений в сфере информационных технологий. Они в свою очередь образуют направления организации работы по защите информации в вычислительных системах.

Для безопасности в сфере информационных технологий необходимо применять средства обеспечения информационной безопасности, которые необходимы для осуществления мер по защите информации, хранящейся как в компьютере, так и в глобальной сети Интернет. Для безопасности своих данных необходимо соблюдать следующие правила:

- при выходе в глобальную сеть Интернет следует использовать средства, на которых предустановлены программы для борьбы с компьютерными вирусами;

- используйте достоверные операционные системы;

- при посещении веб-сайтов обращайте внимание на возможность подделки;

- конфиденциальную информацию необходимо вводить только на тех веб-сайтах, на которых предусмотрена специальная протоколированная система защиты;

- при создании пароля не следует использовать легкую комбинацию, включающую только одни буквы или цифры, необходимо их чередовать;

- дополнительной защитой выступает двухфакторная аутентификация с помощью мобильного устройства;

- предусмотреть возможность подготовки в образовательных организациях МВД России специалистов, способных противодействовать дистанционным хищениям денежных средств граждан;

- организовать на систематической основе курсы повышения квалификации для практических сотрудников, имеющих непосредственное отношение к таким преступлениям;

- предусмотреть в тематических планах по дисциплине «Оперативно-розыскная деятельность» темы занятий, в рамках которых организовать изучение вопросов, связанных с:

а) оперативно-розыскной характеристикой хищений денежных средств граждан, совершенных дистанционно,

б) выявлением, пресечением, предупреждением и раскрытием мошенничеств, совершенных с использованием средств мобильной связи,

в) выявлением, пресечением, предупреждением и раскрытием мошенничеств, совершенных с использованием сети Интернет;

- системно интегрировать в деятельность образовательных организаций МВД России передовой опыт форм и методов оперативно-розыскного противодействия указанным преступлениям, с учетом международного опыта.

Список литературы:

1. Кан Ю. Н. Правовые механизмы и технологии противодействия преступности в сфере информационных технологий // Молодой ученый. 2019. № 45 (283). С. 105.
2. Гурков А.В. Меры безопасности при предотвращении преступлений в сфере информационных технологий // В сборнике: Научный поиск курсантов сборник материалов Международной научной конференции. 2020. С. 37.
3. Попов А.Д. Угрозы и защита информации в автоматизированных системах ОВД как основа предупреждения преступлений в сфере информационных технологий // В сборнике: Перспективы государственно-правового развития России в XXI веке. Сборник материалов Всероссийской научно-теоретической конференции курсантов и слушателей вузов МВД России, студентов гуманитарных вузов, адъюнктов, аспирантов и соискателей. 2017. С. 686.
4. Гайдин А.И. Содержание элемента обстановки в механизме мошенничеств, совершаемых с использованием электронных платежных систем // В книге: Борьба с преступностью: теория и практика Тезисы докладов VII Международной научно-практической конференции. Редколлегия: Ю.П. Шкаплеров [и др.]. 2019. С. 325.