АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Садриддин Шохизиндаев,
Следственное управление при
Главном управлении внутренних дел города Ташкента,
Следственель.

Аннотация:

Мақолада киберхавфсизликка қарши курашнинг долзарб масалалари, шунингдек, виртуал маконда кибер жиноятлар, таҳдидларга қарши курашнинг халқаро ва миллий тажрибаси ўрганилган.

Калит сўзлар: киберхавфсизлик, кибержиноятлар, таҳдид, жаҳон тажрибаси, киберҳужум.

Abst ract:

The article deals with topical issues of countering cybersecurity, as well as international and national experience in combating cybercrime, threats in the virtual space.

Keywords: cybersecurity, cybercrime, threat, world experience, cyberattack.

Аннотация:

В статье рассматриваются актуальные вопросы противодействия кибербезопасности, а также международный и национальный опыт борьбы с киберпреступлениями, угрозы в виртуальном пространстве.

Ключевые слова: кибербезопасность, киберпреступления, угроза, мировой опыт, кибратака.

На сегодняшний день инциденты кибербезопасности происходят во всех секторах экономики и повседневной жизни. Кибербезопасность сегодня неразрывно связана с проявлениями терроризма, мошенничества, вымогательства, а методы защиты от них являются объектом многих научных исследований, проводимых ведущими учеными мира. Киберпространство нуждается в защите, а осуществить его могут только сведущие в данной сфере специалисты, чтобы обеспечить эффективную работу критически важных цифровых инфраструктур как государственного, так и частного сектора.

В мире вопросы кибербезопасности теперь выходят на новый международный уровень. Во всем мире субъекты от отдельных физических лиц до правительства государств прилагают все усилия дабы обеспечить устойчивость киберпространства и зависящих от него систем к кибератакам в условиях постоянного роста масштабов и сложности информационно-коммуникационных сетей, а также огромных объемов данных.

Кибербезопасность – это защита подключенных к Интернету систем, таких как оборудование, программное обеспечение и данные, от киберугроз. Эта практика используется частными лицами и предприятиями для защиты от несанкционированного доступа к центрам обработки данных и другим компьютеризированным системам.

Эффективная стратегия кибербезопасности может обеспечить надежную защиту от вредоносных атак, направленных на доступ, изменение, удаление, уничтожение или вымогательство систем и конфиденциальных данных организации или пользователя. Кибербезопасность также играет важную роль в предотвращении атак, направленных на отключение или нарушение работы системы или устройства.

Внедрение современных информационно-коммуникационных систем в сфере государственного и общественного управления является важным условием эффективной реализации проводимых социально-экономических и общественно-политических реформ и преобразований в стране[1]. Сегодня в стране делается много для эффективного внедрения инноваций, развития новых технологий и инновационных услуг, цифровизации во всех отраслях экономики, повышения технологической культуры и образованности общества. Международный союз электросвязи оценивает приверженность стран делу обеспечения кибербезопасности в связи с чем и был создан Глобальный индекс кибербезопасности, по которому Узбекистан в 2020 году занял 92 место среди 180 стран.

Опыт внедрения ИКТ на примере США, Европейского Союза и Китая, которые применяют различные модели электронного правительства (США – G2B, Евросоюз – G2C, Китай – G2B+G2C), демонстрирует ключевую роль обеспечения информационной безопасности[2].

Как показывает мировая практика и статистика, на сегодняшний день все компании, особенно крупные, финансовый сектор и госучреждения, к сожалению, подвержены риску быть атакованными. По данным интерактивной карты киберугроз лаборатории Касперского, по количеству атак на информационное пространство, по состоянию на 25.11.2020 г. Узбекистан занимает 73 место.

Стоит отметить, что состояние дел в области кибербезопасности зависит от количества и качества кадровых ресурсов, обеспечивающих кибербезопасность, именно поэтому государство должно развивать и наращивать потенциал кадров путем повышения уровня знаний, навыков и умений, необходимых для различных должностей в системе кибербезопасности, а также разработать и осуществить учебные программы и профессиональную подготовку в образовательных учреждениях. Многие страны испытывает нехватку квалифицированных IT-специалистов, исключением не является и наша страна. Несмотря на создание государственного унитарного предприятия «Центра кибербезопасности», создание отдела по борьбе с кибепреступлениями в МВД Республики Узбекистан ощущается явная нехватка квалифицированных специалистов.

Для повышения квалификации специалисты должны проходить переподготовку за рубежом за неимением таковых в республике. В высших военных образовательных учреждениях, к примеру, в Академии МВД нет методического обеспечения по обучения кибербезопасности, а также по расследованию киберпреступлений. Хотя в сентябре 2020 года был создан отдел по расследованию киберпреступлений в Следственном департаменте при МВД

Республики Узбекистан, но методического обеспечения и квалифицированных кадров для качественного производства расследования киберпреступлений и обеспечения кибербезопасности в виртуальном пространстве отсутствует.

Согласно проведенному исследованию одной из распространенных причин уязвимости кибербезопасности, которое приводит к различным кибератакам является: 27% плохая осведомленнолсть пользователей; 26% – нехватка знаний по кибербезопасности, 8% – недостаток финансирования IT решений по кибербезопасности.

В 1985 г. в мире насчитывалось приблизительно 20 тыс. интернет пользователей, жители США составляли 90%. Через 20 лет, в 2005 г., число пользователей интернета по всему миру приблизилось к 1,1 млрд, среди них – более 200 млн американцев (около 17 %). По данным на середину 2013 г. 2,26 млрд человек в мире имеют доступ к интернету с различной степенью охвата населения всемирной паутиной в государствах. Например, в Исландии интернетом пользуется 95% населения, в Германии – 83%, в США – 77,9, в России – 49, в Китае – 38,3%. Несколько иная картина в государствах бывшего СССР. Так, в Эстонии, Латвии и Литве 76,5, 71,7 и 65,1% населения соответственно имеют доступ к интернету; в Азербайджане интернетом охвачены 50% населения, в Казахстане – 45, в Беларуси – 39,6, в Молдове – 38, в Грузии – 36,6, в Украине – 30,6, в Узбекистане – 30,2, в Киргизии – 20, в Таджикистане – 13, в Туркменистане – 5%[3].

В последние годы участились случаи кибератак, что привело к тому, что организации поспешили нанять квалифицированных специалистов, в результате чего на рынке труда стало крайне сложно найти профессионалов в данной сфере. Необходимость и срочность принятия мер усугубляется ситуацией с пандемией COVID-19 и тревожным звонком, вызванным резким увеличением числа успешных кибератак. Обучение и подготовка специалистов в области кибербезопасности не поспевает за необходимостью создания квалифицированной рабочей силы.

Причины этого дефицита многочисленны и разнообразны. На уровне формального образования (университет или колледж) за последние десять с лишним лет число специалистов по кибербезопасности неуклонно росло, но число выпускников все еще не достигает уровня, которого требует отрасль. Для обучения и подготовки высококвалифицированных специалистов требуется много времени, а ещё больше времени необходимо для приобретения ими практического опыта работы. В то же время инвестиции в подготовку кадров по вопросам кибербезопасности серьезно ограничены, поскольку бюджеты по статьям расходов, не связанным непосредственно с прибылью и доходом, были значительно сокращены [4].

Законодательное регулирование вопроса обеспечения кибербезопасности как в государственных и негосударственных учреждениях, так и в виртуальном границах страны, позволит создать качественную методическую базу для обучения и повышения квалификации IT специалистов для решения вопросов кибербезопасности и борьбы с киберпреступностью.

Список литературы:

1. Б.Маниязов. Кибербезопасность: отражение электронных атак. Мнение депутата. 17.12.2020. https://parliament.gov.uz/ru/events/opinion/33101/

2. И.Н. Кохтюлина. Международные аспекты информационной безопасности России в условиях глобализации. Дисс. канд.юрид.наук. Москва. 2010. – С. 3

3. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Отв. ред. М.Б. Касенова; сост. О.В. Демидов и М.Б. Касенова. – М.: Статут, 2013. – С.9

4. Clare Naden. Эдуард Хамфрис. Нехватка знаний в области кибербезопасности. 15 апреля 2021. https://www.iso.org/ru/news/ref2655.html

ПОНЯТИЕ И СУЩНОСТЬ ИНСТИТУТА НАЗНАЧЕНИЯ БОЛЕЕ МЯГКОГО НАКАЗАНИЯ

Миракбар Илмуратов,
Национальная Гвардия Республики Узбекистан,
Капитан, командир группы воинской части № 98157.

Аннотация:

Мақолада энгилроқ жазо тайинлаш институтининг моҳияти ва моҳияти тасвирланган. Шунингдек, мақолада, энгилроқ жазо тайинлаш белгилари таҳлиллари натижаларига асосланган.

Калит сўзлар: тушунча, муассаса, тайинлаш, енгил жазо, жиноят қонунчилиги, инсонпарварлик, фарқлаш, индивидуаллаштириш.

Abstract:

The article describes the concept and essence of the institution of assigning a lighter punishment. Also, in the article, based on the results of analyzes of signs of assigning a lighter punishment.

Key words: Concept, institution, appointment, lenient punishment, criminal legislation, humanization, differentiation, individualization.

Аннотация:

В статье описаны понятие и сущность института назначения более мягкого наказания. Также, в статье на основе результатов анализов признаков назначения более мягкого наказания.

Ключевые слова: Понятие, институт, назначения, мягкого наказания, уголовное законодательство, гуманизация, дифференциации, индивидуализации.

В ходе прогрессивного развития государства на различных этапах его становления перед законодателем стоит задача по решению социальных проблем. Одна из них заключается в охране общества от преступных посягательств, что обеспечивается, в частности, посредством уголовно-правовых мер воздействия.