УДК 343.9

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРЕДУПРЕЖДЕНИЯ КИБЕРПРЕСТУПНОСТИ

Далгалы Татьяна Александровна
канд. юрид. наук
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: tanya.rodionova@gmail.com

Бехре Айдоган
студент
Университет Кырыккале,
г. Анкара, Турция
email: Behrecep2001@gmail.com

Аннотация*: В статье рассмотрен ряд аспектов относительно места цифровых технологий в системе предупреждения киберпреступности. Анализируются возможности цифровых технологий в современной правоохранительной деятельности в целях обеспечения кибербезопасности. Отмечается необходимость использования цифровых технологий в системе предупреждения киберпреступлений.*

Ключевые слова*: цифровые технологии, кибепреступления, кибербезопасность, предупреждение киберпреступности.*

DIGITAL TECHNOLOGIES IN THE CYBER CRIME PREVENTION SYSTEM

Dalgaly Tatyana Aleksandrovna
candidate of legal sciences
Krasnoyarsk state agrarian University,
Krasnoyarsk, Russia
email: tanya.rodionova@gmail.com
Behre Aydogan
student
Kirikkale University,
Ankara, Turkey
email: Behrecep2001@gmail.com

Abstract*:* The article discusses several aspects regarding the place of digital technologies in the cybercrime prevention system. The possibilities of digital technologies in modern law enforcement to ensure cybersecurity are analyzed. The necessity of using digital technologies in the cybercrime prevention system is noted.

Keywords: digital technologies, cybercrimes, cybersecurity, cybercrime prevention.

Защита прав, свобод и законных интересов граждан является одной из самых актуальных и острых проблем как на мировом, так и на общероссийском уровне. Особенно остро эта проблема возникает в связи с беспрецедентным развитием в современном мире цифровых технологий. По данным международных экспертов в мире каждую секунду создаются 4 вредоносных файла, а к 2023 году более 80% людей будут иметь свой аватар в цифровом мире. Столь стремительное развитие цифровых технологий не осталось без внимания преступного сообщества, которое использует все преимущества и недостатки киберпространства для удовлетворения своих преступных целей. Как справедливо отмечает Президент РФ Владимир Путин, «вопрос с кибербезопасностью является одним из самых важных на сегодняшний день» [1].

Кроме того, в феврале 2021 года Президент Российской Федерации заявил о необходимости создания стратегии по борьбе с кибепреступнстью [2]. Думается, что подобные решения главы государства связаны с неприемлемым уровнем преступности в киберпространстве за последние годы. Так, например, согласно официальным данным Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации, только за 2020 год уровень преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации составил 510396 преступлений, что на 73,4% выше предыдущего 2019 года. Более того, только в Санкт-Петербурге рост зарегистрированных преступлений с использованием информационно-телекоммуникационных технологий за 2020 год составил 780,6%. При этом необходимо учитывать, что данная категория преступлений является высоко латентной, поэтому можно только догадываться о том, сколько преступных посягательств осталось за пределами официальной статистики.

Рис. 1 Преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [3]

В докладе Европола 2020 года «Пандемический спекулянт: как преступники эксплуатируют кризис COVID-19» аналитики отмечают, что преступники использовали кризис, просто адаптируя свои способы действий под новые условия. То есть это классические преступления с

новыми параметрами. Ключевым тезисом здесь является вывод о том, что преступники использовали кризис COVID-19 и цифровые технологии для проведения атак с помощью механизма социальной инженерии. То есть получали необходимую конфиденциальную информацию потерпевших (пароли, коды и так далее), используя их доверчивость и неосторожность.

Именно поэтому в целях обеспечения предупреждения кибепреступлений важно обратить внимание не только на обеспечение безопасности цифрового пространства, но и совершенствовать меры виктимологической профилактики, которая позволяет системе предупреждения киберпреступлений быть целостной, завершенной и более эффективной.

В целом, исходя из анализа официальных данных, следует сделать вывод о неизбежности дальнейшего роста киберпосягательств, поэтому так важно доктиринальное осмысление всех происходящих процессов, а также определения перспективных направлений правоохранительной деятельности государства.

Список литературы

1. Путин назвал кибербезопасность одной из важнейших тем современности. Режим доступа: https://tass.ru/politika/11637535
2. Путин призвал создать стратегию по борьбе с киберпреступностью. Режим доступа: https://iz.ru/1128864/2021-02-24/putin-prizval-sozdat-strategiiu-po-borbe-s-kiberprestupnostiu
3. Состояние преступности в России: январь-декабрь 2020. Режим доступа: https://мвд.рф/Deljatelnost/statistics

УДК 340

НОВЫЕ ТЕХНОЛОГИИ В ЮРИСПРУДЕНЦИИ В КОНТЕКСТЕ СОВРЕМЕННЫХ КОНЦЕПЦИЙ ВЛАСТИ

Демина Нина Александровна
канд. филос. наук, доцент
Красноярский государственный аграрный университет,
г. Красноярск, Россия
email: nndeom@mail.ru

Аннотация: *В статье анализируется специфика использования современных информационно-коммуникативных технологий в юриспруденции в свете концепций дисциплинарной власти и биовласти. Рассматриваются особенности использования систем искусственного интеллекта и биометрических систем в юридической сфере.*

Ключевые слова: *дисциплинарная власть, биовласть, искусственный интеллект, информационно-коммуникативные технологии, нейронные сети, биометрия.*