**Философские проблемы информатики. Киберпреступность.**

В статье **[4]** рассказывается о наиболее опасных вирусописателей, которые составляют хакеры-одиночки или группы хакеров, которые создают вредоносные программы, чтобы использовать их в криминальных целях. Эти киберпреступники создают компьютерные вирусы и троянские программы, которые способны:

1) Красть коды доступа к банковским счетам. 2) Рекламировать продукты или услуги на компьютере жертвы. 3) Нелегально использовать ресурсы зараженного компьютера, чтобы разрабатывать и осуществлять сетевые атаки (также называемые DDoS-атаками).

В статье **[7]** дана оценка уровня киберпреступности, обобщён экономический ущерб от таких преступлений. Рассмотрены вопросы противодействия источникам угроз в информационном пространстве в общемировом масштабе. В **[6]** статье под кибербезопасностью понимают защиту от атак в киберпространстве, а под информационной безопасностью ― защиту данных от любых форм угроз, независимо от того, являются ли они аналоговыми или цифровыми, а также рассказывается, что именно входит в сферу интересов кибербезопасности. В статье **[5]** большое внимание уделено вопросам соблюдения прав и свобод граждан в информационной сфере и в обеспечении кибербезопасности. Для широкого круга практических и научных работников, занимающихся вопросами организации борьбы с киберпреступностью и кибертерроризмом, а также для преподавателей, аспирантов и студентов высших учебных заведений.

В статье **[1]** подробно расписано, почему киберпреступления – угроза национальной безопасности. Ситуация с киберпреступностью и кражей денег у населения по телефону с каждым годом лишь ухудшается – власти уже официально признают ее национальной проблемой.

Проблемы кибербезопасности в России раскрывается в статье **[2]** Фактически, сформулированный и закрепленный целостный подход к национальной проблематике кибербезопасности на сегодняшний день отсутствует.

В **[3]** статье выражается потребность в компетенции необходимых специалистов. Когда дело доходит до всех видов киберпреступности, отдельные лица и компании должны сами сообщить об этом полиции, чтобы уменьшить риск и предотвратить проблемы.

Если появились какие-либо подозрения, необходимо немедленно начать внутреннее расследование. Возможно, у вас есть определенные подозрения, но вы не чувствуют себя в состоянии провести расследование, поскольку у вас нет необходимых навыков. Это понятно. Но есть правовые эксперты, которые могут сделать это для вашей компании.

Список литературы:

1. Вадим Арапов. [Почему киберпреступления – угроза национальной безопасности](https://www.vedomosti.ru/technology/articles/2021/12/07/899278-kiberprestupleniya-bezopasnosti). 2021 г.
2. Алина Михайлова. [Проблемы кибербезопасности в России и пути их решения.](https://www.garant.ru/article/520694/) 2014 г.
3. Азизур Рахман. [Киберпреступность - снижение рисков.](https://www.rahmanravelli.co.uk/ru/cybercrime.php) 2023.
4. Евгений Валентинович Касперский. [Киберпреступность и информационная преступность.](https://www.kaspersky.ru/resource-center/threats/cybercrime) 2023.
5. Владимир Овчинский. [Основы борьбы с киберпреступностью и кибертерроризмом.](https://www.labirint.ru/books/680988/) 2017.
6. Positive Research. [Что такое кибербезопасность.](https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost/) 2022.
7. Казимиров Д. А. [Киберпреступность в России и мире: противодействие угрозе современности.](https://www.elibrary.ru/item.asp?id=36945784) 2019.