УДК 343

«Превентивные меры предупреждения правонарушений в сфере информационных технологий»

Четвериков Ярослав Дмитриевич, студент, Красноярский государственный аграрный университет, Красноярск, Россия, e-mail: kaiservondegurechaff1@gmail.com

Барсионов Сергей Александрович, студент, Красноярский государственный аграрный университет, Красноярск, Россия**,** e-mail: barsionov03@gmail.com

Трофимова Светлана Алексеевна, доцент кафедры, кандидат философских наук, Красноярский государственный аграрный университет, Красноярск, Россия, e-mail: kaiservondegurechaff1@gmail.com

Аннотация: развитие информационных технологий и цифровых сервисов дало не только новые возможности для общества и бизнеса, но и новые способы совершения преступлений. С каждым годом правонарушения в киберсфере становятся изощреннее, а ущерб от них всё серьёзнее. Поэтому ключевым направлением является превенция — создание системы мер, которые позволят предупредить угрозы ещё до их реализации.

Ключевые слова: кибербезопасность, правовые риски, превенция, информационные технологии.

"Preventive Measures to Prevent Offenses in the Field of Information Technology"

Chetverikov Y., student, Barsionov S., student, Trofimova S.A., PhD in Philosophy.

Krasnoyarsk State Agrarian University

kaiservondegurechaff1@gmail.com

Abstract: the development of information technologies and digital services has created not only new opportunities for society and business, but also new ways of committing crimes. Every year, cybercrime becomes more sophisticated, and the damage from it is more serious. Therefore, prevention is the key direction — building a system of measures that will prevent threats before they are realized.

Keywords: cybersecurity, legal risks, prevention, information technologies.

Сегодня мы живём во времена, когда информационные технологии стали неотъемлемой частью жизни — через них проходят финансовые операции, государственные услуги, обучение, общение. Но вместе с этим развитие цифровой среды породило новые способы совершения правонарушений, от простого мошенничества в сети до сложных кибератак на государственные и корпоративные ресурсы. Эти преступления наносят ущерб не только отдельным гражданам, но и целым отраслям экономики и государственной безопасности. Именно поэтому на первый план выходит превенция — система мер, направленных на предупреждение правонарушений ещё до того, как они будут совершены.

Характерным примером является недавняя кибератака на компанию «Аэрофлот», что привело к поломке серверной составляющей сети коммуникаций внутри компании, а это в свою очередь к остановке авиасообщений внутри страны. Со слов хакеров, что поделились информацией с журналистами, основным фактором открытия пространства для атаки, на систему Аэрофлота, стал «человеческий фактор», а именно то, что сотрудники пренебрегали правилами безопасности, при работе с компьютерными системами организации[1]. Так же, ещё одним из примером, доказывающим актуальность

[1] Журнал: Lenta.ru // Статья: «Хакеры, заявившие об уничтожении систем «Аэрофлота», раскрыли подробности атаки. Что они сделали?» // URL: https://lenta.ru/news/2025/07/28/nikto-nichego-ne-znaet-stali-izvestny-podrobnosti-masshtabnoy-hakerskoy-ataki-na-aeroflot/

данной проблемы, можно назвать недавнюю DDoS-атаку (DDoS-атака — это отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса – «отказ в обслуживании» или DoS (Denial-of-service))[2] на сеть «Орион телеком», что привело к нарушению работы социальной структуры телекоммуникаций.[3] Анализ экспертов подтверждает слова хакеров о том, что причиной таких инцидентов часто становится халатность сотрудников и отсутствие систематической работы по кибербезопасности. Превентивные меры в таких случаях включают не только технические решения, но и постоянное обучение персонала, введение обязательных стандартов безопасности и ответственности за их нарушение.

Ко всему прочему, можно вспомнить международный случай, что затронул как гос. структуры, так и обычных пользователей. Так, атака вируса-шифровальщика WannaCry в 2017 году, атаковала сотни компаний и государственных учреждений по всему миру, что привело к тому, что часть сетевой инфраструктуры, были парализованы. Причиной распространения вируса, стала элементарная несвоевременность установки обновлений операционных систем. Превентивной мерой в данном случае было бы регулярное обновление программного обеспечения и использование систем резервного копирования, которые позволили бы минимизировать ущерб.[4]

Если же говорить о статистике за последние годы, то нельзя не упомянуть, что в последнее время, наблюдается тенденция спада киберпреступности в Российской Федерации. По данным приведенными пресс-центром МВД,[5] за

[2] Журнал: Kaspersky // Статья: «Что такое DDoS-атака?» // URL: https://www.kaspersky.ru/resource-center/threats/ddos-attacks
[3] Журнал: РБК // Статья: «Крупнейший провайдер Красноярска сообщил о DDoS-атаке» // URL: https://www.rbc.ru/society/12/06/2025/684a56cb9a79471c023aa6d6
[4] Журнал: Kaspersky // Статья: «Крупнейшие угрозы программ-вымогателей» // URL: https://www.kaspersky.ru/resource-center/threats/ransomware-threats-an-in-depth-guide
[5] Редакция CISOCLUB // Статья: «В России зафиксировано снижение IT-преступлений на фоне сохраняющейся высокой доли цифрового мошенничества» // URL: https://cisoclub.ru/v-rossii-zafiksirovano-snizhenie-it-prestuplenij-na-fone-sohranjajushhejsja-vysokoj-doli-cifrovogo-moshennichestva/

первое полугодие 2025 года, по сравнению с прошлым годом количество преступлений в сфере компьютерных технологий идет на тенденцию снижения:

- Преступления в сфере компьютерной информации в первом полугодии 2025 года, уменьшилось в процентном соотношении на 22,3%;

- Отмечается уменьшение краж с использованием дистанционных технологий на 14,3%;

- Доля преступлений с информационно-телекоммуникационными технологиями выросло на 0,7%.

Таким образом, превентивные меры предупреждения правонарушений в сфере информационных технологий нельзя сводить к одному элементу. Они представляют собой комплекс, где правовое регулирование задаёт общие рамки, технические решения обеспечивают защиту, а организационная работа с людьми минимизирует вероятность ошибок. Примеры утечки данных «Аэрофлота» или мировых кибератак показывают, что каждый подобный инцидент мог быть предотвращён, если бы меры превенции применялись системно, а не формально. И подобные с подвижки со стороны государства, мы можем увидеть во вступившем в силу - Федеральный закон от 07.04.2025 N 58-ФЗ "О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации", который ввел дополнительные требования к программным обеспечениям, как например: сведения об этом программном обеспечении должно быть включено в реестр российских программ для ЭВМ и баз данных. Данное изменение должно снизить вероятность проникновения в сеть поскольку, для проникновения в сеть ее необходимо будет изучить, а также, упростит возможности своевременного обновления системы для борьбы с различными уязвимостями.

Таким образом, мы можем увидеть, что только сочетание законодательства, технологий и человеческого фактора может в действительности снизить правовые риски и повысить устойчивость общества к киберугрозам.

Список литературы:

1. Антонян Е.А. Обзор правоприменительной практики по противодействию киберпреступлений / Е.А. Антонян, Е.Р. Россинская, Е.Н. Клещина. - Москва: Консорциум "Инновационная юриспруденция", 2024. - 88 с. / URL: https://consortium.msal.ru/wp-content/uploads/2024/07/K_1-Obzor_Pravoprimenitelnoj-praktiki-po-protivodejstviju-kiberprestuplenij.pdf;

2. В России резко выросло число киберпреступлений // The Moscow Times. - URL: https://www.moscowtimes.ru/2024/05/29/vrossii-rezko-viroslo-chislo-kiberprestuplenii-a132273;

3. Ильницкий А.С. Противодействие криминальной идеологии в сети Интернет: автореф. дисс. Конд. Юрид. Наук. Краснодар, 2022;

4. Журнал Lenta.ru // Статья:» Хакеры, заявившие об уничтожении систем «Аэрофлота», раскрыли подробности атаки. Что они сделали?» // URL: https://lenta.ru/news/2025/07/28/nikto-nichego-ne-znaet-stali-izvestny-podrobnosti-masshtabnoy-hakerskoy-ataki-na-aeroflot/;

5. Журнал: Kaspersky // Статья: «Что такое DDoS-атака?» // URL: https://www.kaspersky.ru/resource-center/threats/ddos-attacks;

6. Журнал: РБК // Статья: «Крупнейший провайдер Красноярска сообщил о DDoS-атаке» // URL: https://www.rbc.ru/society/12/06/2025/684a56cb9a79471c023aa6d6;

7. Журнал: Kaspersky // Статья: «Крупнейшие угрозы программ-вымогателей» // URL: https://www.kaspersky.ru/resource-center/threats/ransomware-threats-an-in-depth-guide;

8. Редакция CISOCLUB // Статья: «В России зафиксировано снижение IT-преступлений на фоне сохраняющейся высокой доли цифрового мошенничества» // URL: https://cisoclub.ru/v-rossii-zafiksirovano-snizhenie-it-prestuplenij-na-fone-sohranjajushhejsja-vysokoj-doli-cifrovogo-moshennichestva/.