

УДК 340

**Лебедев Семен Яковлевич**

Заслуженный юрист РФ,

доктор юридических наук, профессор,

Российский государственный университет имени А.Н. Косыгина

lebesem@yandex.ru

**Джафарли Вугар Фуад оглы**

кандидат юридических наук, доцент,

Российский государственный университет имени А.Н. Косыгина

nizami.66@mail.ru

**Semyon Ya. Lebedev**

Doctor of Law, Professor,

Honored Lawyer of the Russian Federation,

Kosygin Russian State University

lebesem@yandex.ru

**Vugar F. Jafarli**

Candidate of Law, Associate Professor,

Kosygin Russian State University

[nizami.66@mail.ru](mailto:nizami.66@mail.ru)

## **ПЕРСПЕКТИВЫ РАЗВИТИЯ УГОЛОВНО-ПРАВОВЫХ ИННОВАЦИЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ КРИМИНОЛОГИЧЕСКОЙ КИБЕРБЕЗОПАСНОСТИ**

### **PROSPECTS FOR THE DEVELOPMENT OF CRIMINAL LAW INNOVATIONS IN THE SYSTEM OF ENSURING CRIMINOLOGICAL CYBERSECURITY**

***Аннотация.** В статье анализируются перспективы уголовно-правового обеспечения криминологической безопасности в сфере информационных технологий, оценивается роль и место уголовно-правового ресурса в системе обеспечения криминологической кибербезопасности, обосновываются предпосылки цифровизации уголовного закона и определяются условия встраивания уголовно-правовых норм в существующую систему обеспечения кибербезопасности, предлагаются уголовно-правовые меры, направленные на предупреждение инновационных преступлений, совершаемых в киберпространстве, а также традиционных уголовно наказуемых деяний, совершаемых с использованием современных информационных технологий.*

***Ключевые слова:** киберпреступность, криминологическая безопасность, кибербезопасность, цифровой уголовный закон.*

***Abstract.** The article analyzes the prospects of criminal-legal provision of criminological security in the field of information technologies, assesses the role and place of criminal-legal resources in the system of ensuring criminological*

*cybersecurity, substantiates the prerequisites for digitalization of criminal law and defines the conditions for embedding criminal-legal norms in the existing system of ensuring cybersecurity, suggests criminal-legal measures aimed at preventing innovative crimes committed in cyberspace, as well as traditional criminal acts committed using modern information technologies.*

**Keywords:** *cybercrime, criminological security, cybersecurity, digital criminal law.*

Очевидно, что воздействие на криминогенные явления и, как их следствие, - уголовно наказуемые деяния лишь тогда обретет требуемую государством и обществом социально-правовую осмысленность и соответствующую ему результативность, когда оно будет осуществляться системно и комплексно посредством адекватных по степени своего антикриминогенного потенциала и оптимальных по своим ресурсам криминологических, уголовно-правовых, уголовно-процессуальных, криминалистических, оперативно-разыскных и уголовно-исполнительных средств обеспечения социально-правовой защиты личности, общества, государства от преступности. Современная цифровая эпоха, безусловно, добавляет к этому, до недавнего времени, обычному антикриминальному арсеналу, собственные информационно-технологические условия и ресурсы, без которых традиционные средства предупреждения, раскрытия и расследования преступлений, а равно, обращения с преступниками, становятся, мягко говоря, малоэффективными. Потому в условиях беспрецедентного нарастания процессов цифровизации, стремительно поглощающих своим развитием привычные для человека типажи его повседневной деятельности, вполне понятной и обоснованной становится насущная потребность в адекватной современным цифровым угрозам социально-правовой защите существующих и будущих общественных отношений.

Следуя логике цифрового развития систем управления обществом, как нам представляется, в перспективе, любое противоправное деяние должно быть обречено на подверженность адекватной ему форме цифрового правоохранительного реагирования. Можно предположить, что в будущем каждое правонарушение с момента его обнаружения, фиксации и вплоть до снятия или погашения судимости виновному в его совершении лицу, то есть, в течение всего времени, относимого к периоду реализации уголовного судопроизводства, может и должно сопровождаться различными оцифрованными правоохранительными процедурами. На наш взгляд, это максимально приблизит уголовное право и реализующий его уголовный процесс к актуальным информационно-технологическим стандартам социального управления в сфере обеспечения криминологической безопасности.

В данном случае имеется в виду, что каждая стадия, через которую «пропускается» факт правонарушения, должна быть *объективизирована путем цифровизации*. Тем самым, она будет лишена, проявляющейся

сегодня повсеместно в правоохранительной практике субъективно-предвзятой интерпретации реально существующих юридических фактов и событий в чьих-либо, к примеру, личных либо корпоративных корыстных или прочих неправовых интересах.

Подобная цифровая, лишенная тенденциозной человеческой предвзятости, как модель уголовно-правового воздействия на преступления будет способствовать формированию в обществе принципиально новой правовой ментальности. Следуя ей, всякий человек будет стремиться к правопослушному поведению, по максимуму избегая нежелательного контакта с законом, поскольку будет осознавать, что любой его негативный, социально предосудительный шаг отслеживается и юридически должным образом оценивается автоматически. Именно так объективизируется главное, провозглашенное некогда известным итальянским юристом-просветителем Чезаре Беккариа в его бессмертном труде «О преступлениях и наказаниях» (1764 г.): правовое средство удержания от совершения преступления, заключающееся «...не в жестокости наказаний, а в их неизбежности... Уверенность в неизбежности хотя бы и умеренного наказания произведет всегда большее впечатление, чем страх перед другим, более жестоким, но сопровождаемый надеждой на безнаказанность»[1].

Разумеется, реализация предлагаемой идеи сопряжена с множеством сомнений, уже получивших в общественном мнении свое протестное звучание в виде, так называемого, «цифрового концлагеря», дискуссии о котором сегодня становятся в обществе самостоятельным источником нового социального конфликта, главным образом, между правозащитниками и инновационно-информационными технологами[2]. Возможно, в данном случае необходим некий «здоровый» макиавеллизм[3], когда под страхом обнаружения и изобличения со стороны «всевидящего ока», к примеру, видеокамеры, оборудованной функцией искусственного интеллекта, в полной мере будет реализовываться превентивный эффект. Такой вид психологического воздействия нам представляется совершенно необходимым, поскольку для немалого числа сограждан именно страх изобличения при совершении преступления - самый действенный и эффективный способ на пути к правопослушному поведению, как в настоящем, так и в будущем. Но этого явно мало, поскольку недостаточно рассчитывать лишь на страх перед неизбежным наказанием. Ведь нельзя забывать о том, что существует извечное «высшее мерило» - социальная справедливость, к достижению которой должна стремиться всякая власть. Между тем, обеспечить пусть не идеальный, но все же достаточно высокий уровень справедливости при отправлении правосудия в расширяющемся цифровом пространстве традиционным уголовно-правовым правоприменением явно не удастся.

Образно понимая выражение Нила Геймана «Куда бы ты ни поехал, ты берешь с собой себя», мы приходим к выводу: нет и не может быть идеального, абсолютно справедливого следователя или судьи, лишённого всяческого пристрастия, ибо субъективизм - в самой природе человека[4].

Получается, что добиться достижения социальной справедливости «всегда и везде» посредством задействования исключительно человеческого «мерила» вряд ли возможно. Перспектива масштабного решения такой проблемы, на наш взгляд, заключена в разумном и взвешенном применении технологии искусственного интеллекта, способной «выключить» субъективный ресурс и максимально реализовать объективный подход к юридической оценке фактов социальной действительности.

Следовательно, исходя из изложенного и учитывая правоохранительные интересы и чаяния общества, нуждающегося в объективной уголовно-правовой защите от преступных посягательств, сопровождаемой соответствующими объективно настроенными механизмами уголовно-правового судопроизводства, представляется целесообразным формирование такой системы уголовно-правового контроля над преступностью, которая будет способна не только укреплять, прежде всего, в криминогенно ориентированных субъектах ощущение неизбежности наказания за совершение ими преступлений, но, что более важно, способствовать реализации социально значимого принципа справедливости, обеспечиваемого, опять-таки, неотвратимостью наказания.

Разумеется, обеспечение криминологической безопасности связано с комплексом социально-правовых ресурсов, каковые создают систему антикриминального контроля, реализуемого государством и обществом посредством:

- определения закономерностей и тенденций преступности, ее состояний в прошлом, настоящем и будущем, применительно к разным пространствам и временам своих проявлений;
- установления и нейтрализации криминогенных источников правонарушений;
- обнаружения самих фактов правонарушений и, совершающих их правонарушителей, применения в отношении них мер профилактического, административно-правового, уголовно-правового, уголовно-процессуального и уголовно-исполнительного воздействия;
- осуществления постпенитенциарного контроля;
- предупредительной деятельности в отношении потенциальных и реальных потерпевших от преступных посягательств (виктимологической профилактики).

В то же время, учитывая всеобъемлющую информационно-технологическую перспективу развития государственного контрольного ресурса в системе социального управления, весь социально-правовой контроль над преступностью, безусловно, должен предопределяться и сопровождаться, в первую очередь, адекватным объективным, суть - цифровым - уголовно-правовым реагированием на инновационные криминогенные и криминальные проявления, представляющим базовую правовую основу для системного обеспечения криминологической безопасности, в том числе, и в киберпространстве. Воплощение такой идеи

предполагает первостепенное решение следующих научно-практических задач:

1. Формирования, развития и реализации концепции взаимосвязей, взаимозависимостей и взаимодействий международного, правового, правоприменительного, криминологического, информационно-технологического, научно-практического, коммерческого и прочих ресурсов, направленных на обеспечение состояния защищенности личности, общества и государства от посягательств, культивируемых, прежде всего, в киберпространстве с помощью информационных технологий.

2. Оптимизации посредством криминологического и информационно-технологического потенциалов инновационного уголовно-правового ресурса как правовой основы криминологической кибербезопасности, причем, охватывающей полем своего правового контроля не только инновационную преступность в киберпространстве, но и традиционную преступность, культивируемую в обычной (не виртуальной) социальной среде, однако так или иначе связанную с цифровыми технологиями.

3. Встраивания в цифровой потенциал существующего специализированного бизнес-ресурса[5], доказавшего свою результативность в нейтрализации киберугроз, цифровой программы-фильтра, содержащей в качестве контента диспозиции норм Особенной части Уголовного кодекса РФ, позволяющей не просто обнаруживать факты преступлений в киберпространстве, но и одновременно производить их оценку по критерию преступности/непреступности и, соответственно, подвергать таковые объективной уголовно-правовой регистрации.

4. Формирования цифрового ресурса обнаружения и фиксации правонарушений, для чего возможно использование стационарных видеокамер, мобильных цифровых устройств с искусственным интеллектом, беспилотных летательных аппаратов (дронов), оборудованных видеокамерами с функцией распознавания лиц и эмоций, способных не только передавать оперативную картинку, но и преследовать, фиксировать преступников, не исключая, при необходимости, применения инновационных средств обездвиживания таковых до прибытия наряда полиции.

5. Формирования инновационной системы выявления, пресечения и раскрытия преступлений с использованием в оперативно-разыскной деятельности современных цифровых криминалистических средств (форензики), специальных цифровых инструментов негласного получения оперативно-разыскной информации.

6. Формирования инновационной системы предварительного расследования преступлений с применением оцифрованного уголовно-правового ресурса, приобщением к уголовным делам актуальных данных с цифровой диагностической карты (ЦДК), установлением всех объективных обстоятельств по уголовному делу, включая свойства и качества личности обвиняемого.

7. Формирования инновационной системы объективной квалификации и оценки уголовно наказуемых деяний в приговорах с использованием оцифрованного уголовно-правового ресурса, персональных социально-криминологических данных правонарушителей, цифровой системы определения оптимальной меры наказания - «электронные весы правосудия», технологий «блокчейн» в уголовном процессе, иных инновационных технологий в сфере уголовного судопроизводства.

8. Формирования инновационной системы контроля над осужденными во время отбывания ими наказания, при условно-досрочном освобождении, в период судимости, в том числе, в рамках административного надзора с применением видеокамер с функцией распознавания лиц, инновационных средств дистанционного контроля над преступностью.

9. Формирования, развития и постоянной поддержки разнообразных информационных социально-правовых взаимосвязей, взаимозависимостей и взаимодействий на международном и национальном, государственном, общественном и личностном, правовом и правоприменительном, кадровом и образовательном, а также, иных уровнях, способных обеспечивать охрану общественных отношений, а также «на дальних подступах» предвидящих и прогнозирующих криминологические риски и угрозы, в результате чего будет достигнут достаточно высокий уровень предупреждения как инновационной, так и традиционной преступности.

Как нам представляется, решение этих задач предопределено предварительным созданием оптимизированного, в том числе, посредством информационно-технологической трансформации (цифровизации), уголовного закона (*цифрового уголовного кодекса*). По сути, это может быть *первым этапом формирования и развития системы криминологической кибербезопасности*. В свою очередь, процесс такой инновационной трансформации обуславливает решение собственных соответствующих ему теоретических и практических задач:

1. Формулирование понятийного аппарата системы криминологической кибербезопасности.

2. Характеристики и оценки перспектив оптимизации использования уголовно-правового ресурса в обеспечении криминологической кибербезопасности с учетом историко-правового и сравнительно-правового опыта уголовно-правовой охраны общественных отношений от преступлений, совершаемых в сфере информационных технологий.

3. Характеристики и оценки состояния теории и практики уголовно-правовой квалификации преступлений, совершаемых в сфере информационных технологий, а, равно, адекватности уголовно-правовых наказаний за их совершение.

4. Цифрового анализа текста действующего Уголовного кодекса РФ посредством существующих (и специально разрабатываемых) программ искусственного интеллекта на предмет:

а) выявления и устранения в нем несоответствий между уголовно-правовыми запретами и установленными за их нарушения санкциями, с

вероятными общими рекомендациями по поводу оптимального вида и срока уголовного наказания;

б) выявления и устранения логических ошибок, связанных с несоответствиями между утратившими силу и новыми законами;

в) выявления и устранения несоответствий между «материнскими» и специальными составами;

г) выявления и устранения уголовно-правовой тавтологии между различными смежными нормами;

д) выявления и устранения норм-«клонов»;

е) выявления и устранения нечетких понятий;

ж) полноценного учета криминологических свойств и качеств личности преступника при назначении наказания;

з) криминологической обоснованности криминализации и декриминализации преступлений.

5. Обоснования криминологических и информационно-технологических предпосылок оптимизации уголовно-правовой охраны общественных отношений от преступлений, совершаемых в сфере информационных технологий, путей и средств совершенствования соответствующих ей норм уголовного закона.

6. Характеристики современных угроз криминологической кибербезопасности как объектов адекватного и оптимального уголовно-правового контроля и обоснования предпосылок к выработке оптимизированного уголовно-правового ресурса, способного эффективно противостоять как киберпреступности, так и традиционным криминальным посягательствам.

7. Обоснования перспектив информационно-технологической модернизации (цифровизации) уголовного закона и практики его применения в обеспечении криминологической кибербезопасности.

Очевидно, что осуществление процесса «оцифровки» уголовно-правового (кстати, как и иного правового или криминологического) ресурса невозможно без специалистов в области информационных технологий (IT-специалистов). В то же время, ясно, что инициатива подобной цифровизации, безусловно, должна исходить от специалистов в области уголовного права и криминологии. Вместе с тем, существует вполне зримая проблема, заключающаяся в том, что как законодателем, так и рядом специалистов в области уголовного права недооценивается значимость такого феномена, как криминологическая информация, тогда как криминологический материал, связанный с изучением закономерностей киберпреступного поведения, получаемый с помощью таких цифровых технологий, как «большие данные» и «искусственный интеллект», помогающий реализовать познавательный потенциал путем *криминологического кибермониторинга* [6], позволяет объемнее и целенаправленнее создавать актуальные и адекватные существующим криминологическим реалиям системы уголовно-правовых запретов и соответствующих им санкций.

*Вторым предварительным этапом формирования и развития системы криминологической кибербезопасности, целью которого является всесторонний анализ криминологических средств предупреждения преступности в сфере информационных технологий, должна стать оптимизация информационно-технологического и криминологического ресурсов, актуализирующая формирование цифрового уголовного закона и цифровых средств предупреждения преступлений в киберпространстве. На этом этапе предполагается:*

1. Изучение закономерностей, тенденций и состояний преступности и отдельных преступлений в сфере информационных технологий, включая криминологическое прогнозирование киберпреступности.

2. Анализ криминологической (криминогенной и антикриминогенной) детерминации преступности в сфере информационных технологий.

3. Криминологическое моделирование киберпреступлений.

4. Криминологическая характеристика и оценка личности преступника, совершающего уголовно-наказуемые деяния в сфере информационных технологий, а также, оценка места и роли таких преступников в механизмах совершения киберпреступлений.

5. Виктимологическая характеристика и оценка личности потерпевшего от преступлений в сфере информационных технологий, а также оценка места и роли таких потерпевших в механизмах совершения киберпреступлений.

6. Исследование перспектив оптимизации формирования адекватных развитию криминологической ситуации в сфере информационных технологий предметных информационных ресурсов и предметного использования криминологической информации, направленных на обеспечение криминологической кибербезопасности, в том числе с помощью цифровизации предметного для обеспечения криминологической кибербезопасности уголовно-правового ресурса, а именно:

а) осуществление сбора, анализа и определение оценки криминологической информации о состоянии преступности с использованием цифровых технологий и модернизированных с их помощью предметных криминологических и информационно-технологических ресурсов;

б) цифровое оформление информации по уголовным делам, материалам об административных правонарушениях, материалам об отказах в возбуждении уголовных дел, иным материалам (в том числе, по возможности, оперативно-разыскным) и направлением их в единую информационную базу данных о преступности;

в) создание в отношении лиц, склонных к устойчивому антиобщественному поведению, цифровой диагностической карты (ЦДК), формирование и предметное информационное наполнение которой будет осуществляться на всех стадиях допреступного, преступного и постпреступного (в том числе, после отбытия наказаний за совершение преступлений) поведения личности из информационных источников правоохранительных, судебных и иных органов, деятельность которых



связана с индивидуально-профилактическим воздействием в отношении такой личности;

г) цифровизацию информации правового характера, прежде всего, конституционных норм, решений и предписаний Конституционного Суда РФ, рекомендаций международных и отечественных правозащитных организаций, всего массива данных в сфере национального и зарубежного уголовного, уголовно-процессуального и уголовно-исполнительного законодательства, как актуального, так и действовавшего ранее;

д) регулярную оптимизацию формирования, инновационного изменения и дополнения цифровых ресурсов уголовного закона посредством использования технологий больших данных и искусственного интеллекта, с инициацией соответствующих рекомендаций законодателю.

Помимо этого, следует учесть, что, сама по себе, цифровая оптимизация уголовно-правового и криминологического ресурсов является явно недостаточной, поскольку мало создать совершенные цифровые законодательные ресурсы и разработать совершенные, опять-таки, цифровые механизмы их реализации. На наш взгляд, в процесс формирования и развития системы криминологической кибербезопасности необходимо обязательно интегрировать уже существующие или же находящиеся на стадии перспективной разработки иные важные антикриминогенные ресурсы, активно и, главное, результативно реализуемые в современной правоохранительной практике. Таким образом, создается комплексный междисциплинарный ресурс криминологической безопасности (в том числе, кибербезопасности), в котором найдут свое правоохранительное воплощение как специализированные антикриминогенные и антикриминальные, так и иные социально-правовые средства предупреждения преступности. В результате можно вплотную подойти к созданию такого механизма уголовного правоприменения, с помощью которого степень защищенности личности, общества, государства от традиционной или же информационно-технологической преступности будет способна достигнуть желаемого обществом и государством социально приемлемого уровня.

Отмеченное диктует необходимость в реализации *третьего предварительного этапа формирования и развития системы криминологической кибербезопасности – совершенствование комплекса антикриминальных ресурсов*, в рамках которого нам представляется важным произвести:

1. Анализ состояния адекватности и оптимальности соответствия существующих мировых систем правоохранения и позиционируемых ими перспектив своей антикриминогенной деятельности целям криминологической безопасности в сфере информационных технологий, аспектов обеспечения всемерного и полноценного развития предметного международного сотрудничества в этой сфере.

2. Оценку с правовой и информационно-технологической позиций российских отраслевых нормативных правовых ресурсов обеспечения криминологической безопасности в сфере информационных технологий.

3. Изучение научно-практических и инновационно-технологических предпосылок формирования и развития общих нормативных правовых основ системы криминологической безопасности в сфере информационных технологий.

4. Анализ состояния научных, информационно-технологических и коммерческих ресурсов, а также, перспектив привлечения общественного ресурса к обеспечению криминологической безопасности в сфере информационных технологий.

5. Исследование перспектив создания общенациональной системы защиты наиболее важных «сетевых» объектов, образующих критическую информационную инфраструктуру, в качестве которых должны выступать компьютерные группы реагирования на чрезвычайные ситуации - CERT (Computer Emergency Response Team).

6. Инициацию модернизации образовательных стандартов и их реализацию в подготовке, переподготовке и повышении профессиональной квалификации юристов и иных специалистов правоохранительных органов для системы криминологической безопасности в сфере информационных технологий.

7. Оценку перспектив совершенствования предметных антикриминальных (уголовно-правовой, уголовно-процессуальной, криминалистической, оперативно-разыскной и уголовно-исполнительной) нормативных правовых ресурсов, так или иначе связанных с предупреждением преступлений в сфере информационных технологий.

8. Создание системы мониторинга реализации самих цифровых ресурсов обеспечения криминологической безопасности в сфере информационных технологий.

Как нами предполагается, решение перечисленных теоретических и практических задач создаст в перспективе надежную научную основу развития и укрепления системы криминологической кибербезопасности, так необходимой обществу и государству в эпоху цифровых трансформаций общественных отношений.

#### ***Литература:***

1. Беккариа, Чезаре. *О преступлениях и наказаниях* / пер. с фр. А. Хрущов. - СПб. : Тип. И. Глазунова, 1806 / <http://elib.shpl.ru/ru/nodes/57757-bekkaria-ch-o-prestupleniyah-i-nakazaniyah-spb-1806>

2. См. подр.: *Цифровой концлагерь или цифровая утопия. Почему нам всем нужно меняться, чтобы справиться с новыми технологическими вызовами?* – Такие дела, 7 марта 2021 г. / <https://takiedela.ru/>

3. См.: Макиавелли Н. «Государь»: «Что лучше: чтобы государя любили или чтобы его боялись. Говорят, что лучше всего, когда боятся и любят одновременно; однако любовь плохо уживается со страхом, поэтому если уж приходится выбирать, то надежнее выбрать страх» / <https://eksmo.ru/interview/20-tsitat-iz-gosudarya-nikkolo-makiavelli-ID5829868/> (дата обращения: 03.01.2020 г.)

4. См.: Гейман Н. «История с кладбищем»: «Они как те люди, которые думают, что будут счастливы, если переедут в другое место, а потом оказывается: куда бы ты ни поехал, ты берёшь с собой себя» // // <https://www.livelib.ru/book/1001504334/quotes-istoriya-s-kladbischem-nil-gejman> (дата обращения: 10.01.2020 г.)

5. В перспективе, в аналогичный потенциал специализированного государственного ресурса.

6. Более подробно см.: Джафарли В.Ф. О созвучности тезиса «Цифровой безопасности - цифровой уголовно-правовой ресурс» теории криминологической безопасности в сфере информационных технологий / Криминология: вчера, сегодня, завтра. - 2019. № 4 (55). - С. 47-54.

#### **Literature:**

1. Beccaria, Cesare. *On crimes and punishments* / per. with fr. A. Khrushchev. - St. Petersburg: I. Glazunov Type, 1806 / <http://elib.shpl.ru/ru/nodes/57757-bekkaria-ch-o-prestupleniyah-i-nakazaniyah-spb-1806>

2. See sub-section: *Digital concentration camp or digital utopia. Why do we all need to change to meet the new technological challenges?* - *Such Matters*, March 7, 2021 / <https://takiedela.ru/>

3. See: Machiavelli N. "The Sovereign": "Which is better: to love the sovereign or to be afraid of him. They say that it is best to be afraid and love at the same time; however, love does not get along well with fear, so if you have to choose, it is safer to choose fear " / <https://eksmo.ru/interview/20-tsitat-iz-gosudarya-nikkolo-makiavelli-ID5829868/> (accessed: 03.01.2020)

4. See: Gaiman N. "The story of the cemetery": "They are like those people who think be happy if I moved to another place, and then it turns out: wherever you go, you take yourself with you" // // <https://www.livelib.ru/book/1001504334/quotes-istoriya-s-kladbischem-nil-gejman> (date accessed: 10.01.2020 g)

5. In the long term, in a similar capacity of the specialized state of the resource.

6. For more information, see: Jafarli V. F. *On the consonance of the thesis "Digital security - digital criminal law resource" of the theory of criminological security in the field of information technologies* / *Criminology: yesterday, Today, Tomorrow*. - 2019. № 4 (55). - Pp. 47-54.