

Нестеров А.В. О категории уязвимости, в том числе, уязвимости юристов. М.: РФЦСЭ, электронный препринт, февраль 2023. 4 с. URL: [www.nesterov.su](http://www.nesterov.su)

Аннотация. Системы обеспечения безопасности, в том числе, подсистемы юридического обеспечения безопасности, могут обладать уязвимостями, а индивид, которому обеспечивается безопасность – недостатками.

Ключевые слова: недостатки, уязвимости, соотношение, юристы, безопасность, обеспечение.

Система обеспечения национальной безопасности (СОНБ) РФ подразумевает наличие ее подсистемы юридического обеспечения.

Специалисты по обеспечению безопасности используют два понятия, которые называются словами «недостатки» и «уязвимости». К сожалению, часто их рассматривают как синонимы.

Известна классификация уязвимостей информационных систем<sup>1</sup>, в которой дано определение: «уязвимость: Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации».

Отсюда следует, что рассматривается объективная уязвимость для информационной системы в целом, не выделяя подсистему обеспечения безопасности.

Также известен термин «уязвимость юристов», значение которого также необходимо обсудить. В документе<sup>2</sup> отмечено, что юристы могут

---

<sup>1</sup> ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

<sup>2</sup> Отчет ФАТТ. Уязвимости специалистов по правовым вопросам в сфере отмывания денег и финансирования терроризма. Июнь 2013. URL: [https://www.fedsfm.ru/content/files/documents/fatf/ml\\_ft\\_legal\\_professionals.pdf](https://www.fedsfm.ru/content/files/documents/fatf/ml_ft_legal_professionals.pdf)

быть уязвимы, т.к. их могут использовать преступники при осуществлении экономических преступлений, поэтому в экономике возможны уязвимости юристов, с помощью которых преступники могут прикрывать свои преступления. Кроме того, законопослушные профессиональные юристы могут самостоятельно совершать преступления или соучаствовать в преступлении.

Таким образом, негативные субъекты, в частности, криминалитет, используют профессиональных юристов в своих преступных схемах для осуществления определённых юридических операций, а также для получения доступа к специальным юридическим и нотариальным знаниям и опыту, т.е. рассматривается как субъективная уязвимость.

Известен термин «предикатное преступление», который используется для наименования виновно совершенного общественно опасного деяния, запрещенного уголовным законом государства, предшествующего легализации (отмыванию) доходов от такого деяния.

В этом документе отмечены трудности в сборе доказательств при расследовании преступлений, совершенных профессиональными юристами или с их помощью, в виде: неясность и неуверенность в степени конфиденциальности, профессионального иммунитета, профессиональной тайны, сложный и отнимающий много времени порядок изъятия документов у профессиональных юристов и отсутствие доступа к информации о клиентских счетах.

Однако меры административного, дисциплинарного или уголовного преследования, применяемые по отношению к профессиональным юристам, помогают выявлению уязвимостей. Законопослушные юристы уже сами стали распознавать и выявлять попытки использования их услуг в незаконных целях.

К сожалению, в этом документе нет дефиниции термина «уязвимости», поэтому, наверное, с его помощью называются недостатки в юридической деятельности.

## **Соотношение правовых категорий «недостаток» и «уязвимость»**

Любой индивид, в частности, система, находясь в окружении (окружающей среде), которая по определению является негативной, так или иначе, задумывается об обеспечении своей безопасности или системе она требуется. Поэтому различают системы, у которых есть система (подсистема) обеспечения безопасности, и системы без такой подсистемы.

Будем утверждать, что недостаток (ошибка, дефект) может быть в индивиде, которому обеспечивается безопасность, а уязвимость – в подсистеме обеспечения его безопасности. Не всегда использование уязвимости (нарушение подсистемы обеспечения безопасности) приводит к негативу для индивида. Например, получение несанкционированного доступа к зашифрованному сообщению, еще не означает доступ к его семантическому содержанию (информации).

Поэтому подсистема обеспечения безопасности может иметь уязвимость («слабость»), а уровень обеспечения безопасности может меняться от 0 до 1 в относительных единицах. При этом недостатки индивида требуют самостоятельного устранения, которые могут быть связаны с уязвимостями.

Под уязвимостью будем понимать не недостатки в предметной системе (индивиде), а слабости в подсистеме обеспечения безопасности индивида, в частности, в подсистеме юридического обеспечения безопасности, в том числе, с точки зрения человеческого фактора, и которые могут быть использованы и/или способствовать в реализации негативного воздействия на такую подсистему. Отсутствие или слабая подсистема обеспечения безопасности может содействовать появлению уязвимостей.

Уязвимости могут быть объективными и/или субъективными. Субъективная уязвимость возникает, когда субъект умышленно и/или

непроизвольно по недомыслию и/или халатности, совершает действия, приводящее к появлению уязвимости в системе обеспечения безопасности. Объективная уязвимость возникает, если ее не заметили при разработке, эксплуатации и/или аудите системы обеспечения безопасности. Все эти уязвимости также характерны для подсистемы юридического обеспечения системы обеспечения безопасности индивида.

В рамках подсистемы юридического обеспечения безопасности применяются меры по выявлению уязвимостей не только в системе обеспечения безопасности индивида, но и в самой этой подсистеме, т.к. она также может иметь уязвимости. К сферам (областям, местам) появления уязвимостей в подсистеме юридического обеспечения безопасности можно отнести: криминогенные, коррупциогенные и иные сферы с высоким риском нарушения этой подсистемы, области политики безопасности, НПА, (административные регламенты), персонал, в частности, юристов, которые умышленно и/или непроизвольно могут совершать негативные деяния, и/или связи между ними в их окружении.

Кроме того, доктринально-правовая подсистема, включающая в себя правоведов (юристов-ученых), может выполнять функции по выявлению не только уязвимостей в подсистеме юридического обеспечения системы обеспечения безопасности индивида, но и недостатков (юридических, методологических, терминологических, логических и т.д.) в юридической (законодательной и/или юрисдикционной, а также надзорной) системе РФ.

Таким образом, можно говорить об юридическом обеспечении безопасности субъективных свобод персон (человека и гражданина), юридико-инструментальных прав и/или объективных интересов юридических субъектов (персоны, юридического лица и/или органа публичной власти) и в целом государства.

Выводы. Системы обеспечения безопасности, в том числе, подсистемы юридического обеспечения безопасности, могут обладать уязвимостями, а индивид, которому обеспечивается безопасность – недостатками.