УДК 347.78.025

# БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ БАЗЫ ДАННЫХ ГОСУДАРСТВЕННОГО ЗЕМЕЛЬНОГО КАДАСТРА УКРАИНЫ

**Андрей ПЕТРЕНКО,**
соискатель кафедры интеллектуальной собственности юридического факультета
руководитель отдела издательского и методического обеспечения учебного процесса юридического факультета
Киевского национального университета имени Тараса Шевченко

**АННОТАЦИЯ**

В статье очерчены современные угрозы безопасности функционирования базы данных Государственного земельного кадастра Украины. Определено, что данные угрозы можно разделить на внутренние и внешние, а также обусловленные человеком и вызванные деструктивными природными воздействиями. Особое внимание автор уделяет анализу угроз информационной безопасности функционирования базы данных Государственного земельного кадастра, а также существующих юридически определённых и технологически обоснованных мер предупреждения и противодействия данным угрозам.

**Ключевые слова:** база данных, безопасность, Государственный земельный кадастр, защита авторского права, информационная безопасность, информация, угрозы безопасности.

## FUNCTIONING SECURITY OF THE LAND REGISTER OF UKRAINE

**Andrey PETRENKO,**
Applicant of the Department of Intellectual Property of the Faculty of Law of Kyiv National Taras Shevchenko University,
Head of the Department of Publishing and Methodical Services for Studying Process on the Faculty of Law
of Kyiv National Taras Shevchenko University

**SUMMARY**

This article describes nowadays problems of national security concerning the database of Lands Register of Ukraine. In this research author divides security risks into internal and external, and by the factor of risk into caused by people or destructive natural influences. Most attention in article paid to the IT security threats in functioning of Lands Register of Ukraine, as well as to legally determined and technologically determined actions in case of counteracting described security threads.

**Key words:** database, security, Land Register of Ukraine, security threads, copyright protection, informational security, information.

**Постановка проблемы.** Учитывая тот факт, что информация в условиях становления информационного общества в Украине становится важным объектом гражданско-правовых отношений, закономерным образом происходит и увеличение её объёма, актуализируются потребности её структурирования, безопасного использования и монетизации, урегулирования правовых отношений по поводу информации в целом [1, с. 35–36]. При этом важным инструментом структурирования информации являются базы данных, которые в широком смысле можно рассматривать в качестве компиляции информации, собранной и дифференцированно структурированной.

Очевидные преимущества использования информации, хранящейся в базах данных, обусловило то, что за последние годы базы данных как объекты авторского права, которые динамичным образом эволюционируют, всё чаще используются государственными органами Украины для оптимизации реализации собственных функций (примером этому является база данных Государственного земельного кадастра), что вполне соответствует идеи Стратегии развития информационного общества в Украине, Стратегии реформирования государственного управления Украины на 2016–2020 годы, а также Стратегии реформирования системы управления государственными финансами на 2017–2020 годы.

Тот факт, что базы данных содержат ценную информацию, объясняет, что в течение всего жизненного цикла этих баз (как и любых информационных систем, в основе которых лежит реляционная система управления базами данных) в отношении них могут возникать и реализовываться угрозы различных классов, которые, как правило, закономерным образом обусловлены следующим: 1) жаждой злоумышленников нелегально завладеть соответствующей ценной информацией [2, с. 69]; 2) тем, что базы данных не всегда функционируют в условиях эффективного технического контроля, что обуславливает сбои в их работе и т. п. Благоприятные условия для реализации указанных рисков также обусловлены несовершенством гражданского законодательства в части регулирования баз данных. Между тем, проблемы безопасности баз данных на сегодняшний день остаются недостаточно исследованной темой, а вопросы безопасности базы данных Государственного земельного кадастра (далее – ГЗК) вообще не были предметом комплексного исследования.

**Актуальность темы исследования.** Актуальность данного вопроса выражается в том, что повреждение и неправильное использование информации в базах данных, как отмечают Э. Бертино (Elisa Bertino) и Р. Сандху (Ravi Sandhu), затрагивают права, интересы не только какого-то конкретного пользователя или вредят нормальному функционированию какого-то приложения, но также могут иметь катастрофические последствия для всей организации,

которая владеет этой базой данных [3, с. 2]. Куда более масштабные катастрофические последствия эти угрозы обусловливают случаями их реализации в отношении баз данных государственных органов, а главным образом – базы данных ГЗК, учитывая назначение и цель функционирования данной базы данных, её роль в осуществлении множественных гражданско-правовых отношений в государстве.

**Состояние исследования.** Хотя проблематика угроз безопасности функционирования баз данных ГЗК, а также юридически определённых и технологически обоснованных мер предупреждения и противодействия данных угроз до сих пор комплексно не исследовалась украинскими учёными, обратим внимание на то, что учёными комплексно исследовались угрозы безопасности функционирования баз данных (как таковых), а также отдельные вопросы обеспечения безопасности ГЗК (например, С.А. Миценко, В.А. Некрасов, И.А. Опенько, А.С. Осьмак, Н.М. Пантелеева, Б.О. Пивэнь, А.Я. Сохнич, Р.В. Чернолуцкий, С.А. Чукут и другие ученые).

**Цель и задача исследования.** Учёт важных научных наработок, сформулированных указанными выше учёными, поможет достичь цели и задач научной работы, а именно – определить основные угрозы безопасности функционирования баз данных ГЗК.

Кроме того, достижению указанной цели будет способствовать анализ действующего законодательства Украины, а также выполнение следующих *задач*: 1) определить сущность понятий «угроза», «безопасные условия», а также концептуализировать термин «безопасность функционирования базы данных»; 2) структурировать основные угрозы безопасности функционирования базы данных ГЗК, а также проанализировать существующие юридически определённые и технологически обоснованные меры предупреждения и противодействия данным угрозам.

**Изложение основного материала.** В широком смысле под понятием «угроза» учёными [4, с. 42] понимается потенциально возможное событие (или явление), действие (или процесс), с помощью которых может быть нанесён ущерб интересам субъекта. Соответственно, условия, в которых угрозы интересам субъектов не могут быть реализованы, понимаются в качестве безопасных условий для соответствующих интересов, а обеспечение этих условий – процесс обеспечения безопасности этих интересов. Указанные выводы применимы по отношению к безопасности функционирования баз данных, что подтверждают также и учёные, в той или иной степени рассматривающие данный вопрос. В частности, В.М. Илюшечкин полагает, что безопасность базы данных состоит в защите базы данных от несанкционированного доступа со стороны пользователей [5, с. 19]. Более уточнено этот подход к пониманию безопасности базы данных (*database security*) в трудах зарубежных учёных [см., напр.: 3, с. 2]. В частности, из научных разработок Э. Бертино и Р. Сандху следует, что безопасность базы данных выражается в нормальном функционировании данной базы, а именно в результате соответствия процесса обеспечения указанной безопасности следующим трём требованиям: 1) невозможность несанкционированного вскрытия секретных или конфиденциальных данных, содержащихся в базе данных; 2) незыблемость целостности базы данных через невозможность осуществления несанкционированного и ошибочного изменения информации в базе данных; 3) невозможность искажения уровня доступности базы данных, в частности, путём оперативного исправления сбоев в работе системы и блокирование воздействия на систему управления базой данных (далее – СУБД) вредоносных программ [3, с. 2]. Впрочем, следует отметить, что безопасность базы данных (а именно её функционирования) не должна отождествляться только с достаточным уровнем её защищённости от несанкционированного доступа со стороны пользователей (и/или ненадлежащего администрирования), ведь, как мы уже выше отмечали: 1) безопасность – это противоположность угрозе; 2) угроза проявляется не только в действии, но и в процессе, события и явлении.

То есть под «*безопасностью функционирования базы данных*», по нашему мнению, следует понимать характеристику условий и состояния функционирования базы данных, указывающую на практическое предотвращение реализации угроз функционирования баз данных в виде возможных действий (или событий), процессов (или явлений), с помощью которых может быть искажена цель функционирования базы данных, обусловлена её недостижимость, нанесён ущерб интересам субъекта авторского права на базу данных, а также пользователей базы данных. Учитывая это, приходим к выводу, что многоаспектность угроз функционирования базы данных обуславливает многоаспектность понимания безопасности функционирования этих баз данных, а именно: безопасности функционирования базы данных от *неправомерного* (или *ненадлежащего*) *антропогенного воздействия* или *деструктивного природного воздействия* (метеорологического и агрометеорологического характера, в частности, бури, ураганы, смерчи, сильная жара или сильные морозы и т. д.).

Учитывая позиции учёных [см., напр.: 6–8], которые в своих научных исследованиях уже рассматривали вопрос рисков функционирования баз данных, отметим, что к основным рискам функционирования базы данных ГЗК следует относить следующие:

1) наличие чрезмерных привилегий (*excessive privileges*) в пользовании базой данных. Пользователями базы данных ГЗК являются физическое или юридическое лицо, пользующееся сведениям ГЗК и/или осуществляющее обмен сведениями в порядке информационного взаимодействия между кадастрами, реестрами и информационными системами в соответствии с законодательством. Безопасность базы данных рассматриваемой единой государственной геоинформационной системы сведений о земле обеспечивается объективно необходимыми привилегиями пользователей этой базы данных, которые являются неодинаковыми и зависят от типа пользователя. Указанное основывается на правиле,

установленном в ч. 1 ст. 38 Закона Украины «О ГЗК», сквозь призму которого можно сделать вывод, что привилегии пользователей базы данных ГЗК целесообразно делить на две основные группы: держательские привилегии; привилегии режима чтения;

2) «входная инъекция» (*input injections*). Следует обратить внимание на то, что, посещая сайт «Публичная кадастровая карта Украины», можно сразу же заметить, что на нём расположено сообщение, в котором отмечается, что Держгеокадастром до сих осуществляются меры по исправлению ошибок, которые содержатся в ГЗК. Обозначенные проблемы, как отмечают учёные, являются условиями для того, чтобы злоумышленники осуществляли хакерские атаки на ГЗК, в частности, переписывая данные в соответствующей базе данных, несанкционированным образом изменяя как границы земельных участков, так и их владельцев. Впрочем, данная проблема на сегодняшний день эффективно решается благодаря современным технологиям, среди которых особенное место занимает *Blockchain*, под которым учёные понимают «способ хранения данных или цифровой реестр транзакций, соглашений, контрактов и любых данных, требующих использования отдельных независимых записей» [9, с. 59]. Иными словами, данная технология также является «базой данных для записи и хранения данных о транзакции», одна из главных особенностей которой состоит в том, что она одновременно сохраняется на множестве компьютеров, соединённых друг с другом сетью Интернет. Все изменения в базе данных одного компьютера сразу копируются на каждый компьютер, подключённый к сети. База данных записывает информацию о транзакциях, что условно называется «слоями», а потому, дабы подделать сохранённую информацию, необходимо подделать все верхние «слои», что практически невозможно.

Вместе с тем существенным недостатком внедрения в Украине *Blockchain*-технологий является то, что до сих пор её использование остаётся ещё должным образом не урегулированным. Учитывая это, вне сомнения, снижается уровень однозначности понимания использования указанной технологии, на которой функционирует база данных ГЗК;

3) вредоносное программное обеспечение, используемое против СУБД. Достижение соответствующего уровня безопасности базы данных ГЗК предполагается, среди прочего, в комплексе императивных требований к автоматизированному рабочему месту пользователя ГЗК и надлежащего программного обеспечения;

4) недостаточность аудита (*weak audit trail*). Уровень качества аудита базы данных ГЗК значительным образом повысился в связи с переводом ГЗК на технологию *Blockchain*. Указанное объясняется тем, что четыре ноды находятся у Минагрополитики Украины и одна нода у аудитора – *Transparency International*. Таким образом, данная международная неправительственная организация стала первой общественной организацией, которая получила ноду-аудитора, являющуюся независимым компонентом *Blockchain*, выполняет непрерывный аудит всех транзакций сети блокчейн ГЗК. То есть уровень достаточности аудита базы данных ГЗК как гарантия обеспечения безопасности её функционирования достигается как путём внутреннего аудита по данным ГЗК, так и за счёт публичного онлайн-контроля за реестром;

5) незащищённость резервных копий информации, находящихся в базе данных. Указанная проблема сегодня решена относительно базы данных ГЗК в связи с переходом на технологию *Blockchain*, которая, как мы уже отмечали, позволяет безопасно функционировать базе данных, исключая вероятные искажения информации, находящейся в данной базе, и похищение этой информации.

Таким образом, рассмотрев угрозы информационной безопасности функционирования базы данных ГЗК, можно сделать вывод, что указанные угрозы можно разделить на две группы: 1) внешние информационные угрозы, т. е. те угрозы, которые выражены в несанкционированном посягательстве на базу данных и осуществляемые законными или незаконными пользователями; 2) внутренние (организационные) информационные угрозы, т. е. угрозы, обусловленные ненадлежащими действиями держателя и администратора базы данных. При этом, как следует из изложенного, внутренние угрозы функционирования базы данных в большинстве случаев связаны с увеличением уязвимости базы данных относительно внешних угроз (в частности, это проявляется в ненадлежащем администрировании). Однако подчеркнём, что увеличением уязвимости базы данных внутренние угрозы не исчерпываются.

В очерченном смысле обратим внимание на то, что переход в 2017 году ГЗК на технологию *Blockchain*, бесспорно, позволил снизить уровень уязвимости соответствующей базы данных, однако данный уровень уязвимости был снижен преимущественно перед внешними угрозами функционирования базы данных ГЗК. Необходимо согласиться с теми специалистами, которые утверждают, что «потенциальная подделка данных – не основная проблема кадастра и системы торгов». Следовательно, необходимо иметь в виду, что *Blockchain* не способен помочь нормальному функционированию базы данных ГЗК, «если в систему внесены заведомо неточные данные» [10, с. 74], ведь указанная технология помогает обеспечить неизменность, а не истинность информации в базе данных. Кроме того, важно понять, что сама по себе информация, занесённая в *Blockchain*-реестры, не может считаться достоверной в практической действительности. Это подтверждается сообщением на сайте «Публичная кадастровая карта Украины», в котором, как мы уже отмечали, сообщается о том, что по сей день Держгеокадастром осуществляются меры по исправлению ошибок, которые содержатся в ГЗК.

Кроме того, следует обратить внимание на то, что безопасность функционирования базы данных ГЗК, как мы уже отмечали, не только сводится к минимизации несанкционированных угрожающих действий, но и выражается в защите этой базы от событий, явлений,

процессов, угрожающих функционированию ГЗК. При этом, хотя в нормативно-правовых актах, регулирующих те или иные аспекты функционирования базы данных ГЗК не содержится конкретных правил обеспечения безопасного функционирования этой базы данных от деструктивных природных угроз, следует иметь в виду, что на противодействие данной угрозы направлено администрирование ГЗК, которое осуществляется, среди прочего, с целью обеспечения функционирования соответствующих систем и комплексов мониторинга, безопасности и сигнализации (сигнализации о возникновении нештатных и аварийных ситуаций).

**Выводы.** Контроль функционирования базы данных ГЗК должен быть направленным на достижение безопасности функционирования данной базы. При этом безопасность ее функционирования достигается, прежде всего, путём предотвращения, противодействия и минимизации (т. е. путём применения юридически определённых и технологически обоснованных мер предупреждения и противодействия) реализации различных типов угроз данному функционированию, а именно: рисков антропогенного воздействия, проявляющихся во внешнем и внутреннем воздействии на базы данных; деструктивного природного воздействия (в результате стихийных бедствий, которые вредят нормальному функционированию СУБД).

**Список использованной литературы:**


1. Гладкий В.В. Концептуалізація інформатизації про стан корупції у державних органах України. *Правові засади організації та здійснення публічної влади*: зб. тез Всеукр. наук.-практ. інтернет-конф. (м. Хмельницький, 23–30 квітня 2018 р.). Хмельницький: Вид-во Хмельн. ун-ту управл. та права, 2018. С. 35–38. DOI: 10.5281/zenodo.1205237.

2. Pevnev V., Kapchynskyi S. Database security: threats and preventive measures. *Advanced Information Systems*. 2018. Vol. 2. No. 1. P. 69–72. DOI: 10.20998/2522-9052.2018.1.13.

3. Bertino E., Sandhu R. Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing*. 2005. Vol. 2(1). P. 2–19. DOI:10.1109/TDSC.2005.9.

4. Антонюк А.О., Жора В.В. Загрози інформації і канали витоку. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2001. № 1. С. 42–46.

5. Илюшечкин В.М. Основы использования и проектирования баз данных: учебник. Москва: Изд-во «Юрайт», 2014. 214 с.

6. Chandrashekhar A.M., Ahmed S.T., Rahul N. Analysis of Security Threats to Database Storage Systems. *International Journal of Advanced Research in data mining and Cloud computing*. 2015. Vol. 3(5). P. 18–23.

7. Mariuţa Ş. Principles of security and integrity of databases. *Procedia Economics and Finance*. 2014. No. 15. P. 401–405. DOI: 10.1016/S2212-5671(14)00465-1.

8. Trivedi D., Zavarsky P., Butakov S. Enhancing Relational Database Security by Metadata Segregation. *Procedia Computer Science*. 2016. Vol. 94. P. 453–458. DOI:10.1016/j.procs.2016.08.070.

9. Карпенко О.В., Осьмак А.С. Використання блокчейн-систем органами публічної влади: український та зарубіжний досвід. *Актуальні проблеми державного управління*: зб. наук. пр. ОРІДУ / Голов. ред. М.М. Іжа. Вип. 1 (73). Одеса: Вид-во ОРІДУ НАДУ, 2018. С. 57–62.

10. Чукут С.А., Буряченко К.О. Блокчейн, чи система електронного документообігу: сучасні тенденції впровадження в органах виконавчої влади України. *Інвестиції: практика та досвід*. 2018. № 1. С. 70–76.


ИНФОРМАЦИЯ ОБ АВТОРЕ


**Петренко Андрей Валериевич** – соискатель кафедры интеллектуальной собственности юридического факультета Киевского национального университета имени Тараса Шевченко, руководитель отдела издательского и методического обеспечения учебного процесса юридического факультета Киевского национального университета имени Тараса Шевченко


INFORMATION ABOUT THE AUTHOR


**Petrenko Andrey Valeriyevich** – Applicant of the Department of Intellectual Property of the Faculty of Law of Kyiv National Taras Shevchenko University, Head of the Department of Publishing and Methodical Services for Studying Process on the Faculty of Law of Kyiv National Taras Shevchenko University

*petrenko_av@univ.net.ua*