# Вопросы кибербезопасности в системе внутреннего аудита

***Степанян Сона Г.***
*Аспирант Кафедры Управленческого Учета и Аудита АГТУ*
*Преподаватель финансово-экономического колледжа АГЭУ (Ереван, РА)*
sona.stepanyan96@mail.ru

**УДК:** 657.6:004.056; **EDN:** LRMIBU; **JEL:** M15, L86
**Ключевые слова.** информационная безопасность, аудит информационных технологий, оцифровка, внутренняя проверка, кибератаки

## Ներքին աուդիտի համակարգում կիբերանվտանգության խնդիրները

***Ստեփանյան Սոնա Գ.***
*ՀՊՏՀ կառավարչական հաշվառման և աուդիտի ամբիոնի ասպիրանտ*
*ՀՊՏՀ ֆինանսատնտեսագիտական քոլեջի դասախոս (Երևան, ՀՀ)*
sona.stepanyan96@mail.ru

**Ամփոփագիր.** Թվային աշխարհում վերափոխումները ընկերություններին դրդել է թվայնացնել իրենց գործընթացները, օգտագործել ծրագրային ապահովում և Տեղեկատվական Տեխնոլոգիաների (ՏՏ) գործիքներ՝ նախկինում ձեռքով եղած գործընթացները ավտոմատացնելու համար: Թվայնացված գործիքներով աշխատանքի առավելությունները շատ են՝ սկսած ծախսերի խնայողությունից և արդյունքում շահույթի ավելացումից մինչև աշխատանքի արդյունավետություն, քանի որ աշխատակիցները կարող են հրաժարվել ամենաօրյա միօրինակ գործերից և ավելի շատ ժամանակ հատկացնել ստեղծագործ աշխատանքին: Սակայն նոր թվային նորորարությունների ներդրումը իրենից ենթադրում է մասնագետների վերապատրաստում, կամ նոր մասնագետների ներգրավում կազմակերպություն, ինչը ևս պահանջում է ժամանակ, ֆինանսական միջոցներ, և առաջացնում է մի շարք սպառնալիքներ՝ կապված տեղեկատվական տեխնոլոգիաների անվտանգային կիրառության հետ: Այնուամենայնիվ թվային անվտանգության բարելավումը շատ ընկերություններում առկախ խնդիրներից մեկն է: Կիբեր միջադեպերի աուդիտորները դառնում են կիբեր հարձակումների լավագույն պաշտպանողները՝ սահմանելով արձագանքման և վերականգնման պլաններ՝ նվազագույնի հասցնելու ռիսկը: Կիբերանվտանգության հարձակումներն ավելանում են՝ օգտագործելով ցանցային համակարգերի և սարքերի խոցելիությունը: Հարձակումները գնալով ավելի բարդ են, սպառնացող տեխնոլոգիաներ հանցավոր ձեռնարկությունների, պետության կողմից հովանավորվող հաքերների և այլոց կողմից չարամիտ մտադրություններով: Այս համատեքստում կազմակերպությունները պետք է իրականացնեն կիբեր միջադեպերի արձագանքման և վերականգնման աուդիտ կամ ներքին աուդիտի համակարգում վերահսկողությունը ավելի ուժեղացնեն կիբեր սպառնալիքներից խուսափելու համար:
**Հանգուցաբառեր՝** տեղեկատվական անվտանգություն, տեղեկատվական տեխնոլոգիաների աուդիտ, թվայնացում, ներքին ստուգում, կիբեր հարձակումներ

## Cyber security Issues in the Internal Audit System

***Stepanyan Sona G.***
*PhD student of ASTU Department of Management Accounting and Auditing*
*Lecturer of ASUE College of Finance and Economics (Yerevan, RA)*
sona.stepanyan96@mail.ru

**Abstract**. The transformation in the digital world has pushed companies to digitize their processes, use software and Information Technology (IT) tools to automate previously manual processes. The benefits of working with digital tools are many, from cost savings and resulting increased profits to work efficiency, as employees can ditch the monotonous daily tasks and spend more time on creative work**.** However, the implementation of new digital innovations implies the training of specialists, or the involvement of new specialists in the organization, which also requires time, financial resources, and causes a number of threats related to the security application of information technologies. However, improving digital security is one of the pressing issues in many companies. Cyber incident audits become the best defense against cyber attacks by establishing response and recovery plans to minimize risk. Cyber security attacks are increasing by exploiting vulnerabilities in network systems and devices. Attacks are increasingly sophisticated, threatening technologies from criminal enterprises, state-sponsored hackers and others with malicious intent. In this context, organizations should conduct cyber incident response and recovery audits or strengthen controls in the internal audit system to avoid cyber threats.
**Keywords:** information security, information technology audit, digitization, internal audit, cyber attacks

Понятие «аудит информационной безопасности» уже очень популярно в системе аудита. Это общий термин, который охватывает широкую область проверок. Аудит информационной безопасности призван предотвратить несанкционированный доступ, найти проблемы в системе

безопасности организации, от утечки информации через сотрудников с помощью социальной инженерии до различных кибератак на ИТ-инфраструктуру.

По мнению внутренних аудиторов, они считаются одним из самых больших бизнес-рисков. Аудиторы знают, как все организации реагируют на такие кибератаки, и могут понять разницу между небольшим инцидентом безопасности и крупной катастрофой, поэтому они регулярно выбирают их для внутренних аудитов. Аудит системы реагирования [**4**]. Аудит системы реагирования на киберинциденты и восстановления – очень сложная задача, научиться оценивать кибербезопасность и информационные технологии – все равно что начать новую базу знаний. Для аудиторов важно предпринять следующие начальные шаги, чтобы начать работу и делать то, что лучше всего удается внутреннему аудиту: небольшое домашнее задание и хорошие вопросы. Однако в надежде облегчить эту задачу Институт внутренних аудиторов выпустил новое руководство, которое бесплатно доступно для членов Института внутреннего аудита. Руководство, являющееся частью Руководства по глобальному технологическому аудиту IIA или серии GTAG, охватывает риски и средства контроля, связанные с функциями «Ответ» и «Восстановление» NIST CSF. GTAG предоставляет обзор всех аудиторских рисков и средств контроля для поддержки внутреннего аудита, планирования аудиторских заданий и регистрации объема работ. Делаются ссылки на внешние системы контроля, которые при эффективном использовании могут помочь в разработке проницательных подходов к аудиту. Это руководство поможет внутренним аудиторам [**2**]

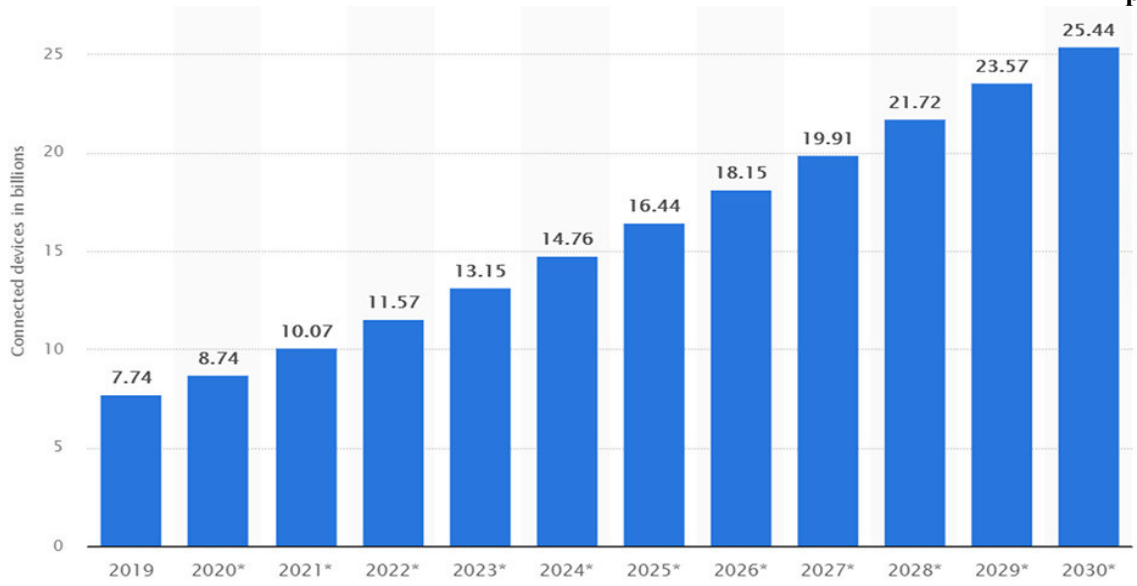
- Определить реагирование на кибер-инциденты и восстановление.
- Развить практические знания о соответствующих процессах, включая управление и управление рисками [**2**].

Понимать риски и возможности, связанные с реагированием на кибер-инциденты и восстановлением.

- Определить компоненты реагирования на кибер-инциденты и восстановления, включая управление, управление рисками и
- Надзор за тестированием и внедрением процессов планирования, а также планов реагирования и восстановления.
- Рассмотрите соответствующие руководящие принципы контроля в рамках широко используемых структур IT-IS, чтобы повысить ценность гарантий и консультационных услуг, предоставляемых службой внутреннего аудита.
- Понимать основы реагирования на кибер-инциденты и аудита восстановления, включая конкретные средства контроля, которые необходимо оценить.
- Защита от киберинцидентов
- Элементы управления реагированием на кибер-инциденты и восстановлением защищают конфиденциальность, целостность и доступность систем и данных, обеспечивая критические уровни для стратегии глубокоэшелонированной защиты.

Поиск и оценка киберрисков очень важны в системе кибербезопасности. Все компании самостоятельно выполняют свою работу через цифровые устройства, а мировой анализ показывает, что к Интернету подключены миллионы устройств.

**График 1**



Согласно изображенному графику, к 2025 году количество подключенных к Интернету устройств превысит 15 миллиардов, а к 2030 году – 25 миллиардов. Глядя на эту картину, становится понятно, что грядущие риски будут более четко видны в цифровом мире, потому что в цифровом мире есть и свои недостатки. Перед системой внутреннего аудита обычно ставится задача изучить и определить, были ли планы реагирования и восстановления разработаны и реализованы эффективно, чтобы обеспечить своевременное восстановление обслуживания [**5**]. Однако прогнозирование кибератак и снижение рисков не гарантируются на 100%, поскольку кибератакам подвержены даже самые влиятельные организации в мире. В 2021 году технологические компании были обеспокоены кибератакой на ИТ-провайдера SolarWinds, компанию, которая стала жертвой сложной и целенаправленной кибератаки, осуществленной иностранным государством. Важность этого дела заключается в том, что клиентами SolarWinds являются большинство крупнейших компаний США, а также правительственные организации, такие как НАСА, ВВС или Пентагон. И если это может случиться с такой ведущей технологической компанией, как SolarWinds, что может случиться с такой компанией, как ваша. Оцифровка процессов и сервисов также сопровождается новыми рисками: кибератаками, угрозами и нарушениями безопасности в системах, которые хакеры и киберпреступники могут использовать для проникновения в базы данных и извлечения информации из компьютерных систем.

**Заключение.** В эту эпоху постоянно растущих и развивающихся информационных технологий важно уделять большое внимание термину кибербезопасность. Потому что даже самые сильные организации в мире не застрахованы от него и, имея самую мощную систему контроля в системе внутреннего аудита, могут быть подвержены кибератакам. Поэтому в статье подробно описаны проблемы, существующие на сегодняшний день при использовании цифровых инноваций, и то, как организации могут снизить свои риски при использовании информационных технологий. Можно сказать, что наиболее важных из них три. Организация не должна предоставлять своим работникам льготы, в которых они не нуждаются при выполнении своей работы. Обеспечение контроля кодов доступа также очень важно, и, что наиболее важно, необходимо обеспечить эффективное разделение обязанностей и ответственности. Таким образом, необходимо реализовать различные уровни ИТ-безопасности на основе тщательной оценки рисков. Эта оценка включает в себя выявление киберугроз, которым подвергается организация, оценку их потенциального воздействия и вероятности возникновения и, наконец, разработку и внедрение средств контроля.

**Перечень использованной литературы**


1. **Schatz Daniel** (2017): «Towards a More Representative Definition of Cyber Security»: Journal of Digital Forensics, Security and Law
2. «Global Cybersecurity: New Directions in Theory and Methods»: Politics and Governance: 2018-06-11: doi:10.17645/pag.v6i2.1569
3. «Computer Security and Mobile Security Challenges»: researchgate.net: 2015-12-03
4. **Butterfield Andrew, Ngondi Gerard Ekembe, Kerr Anne, eds.**: (2016-01-21): A Dictionary of Computer Science: Oxford University Press: ISBN 9780199688975:
5. **Lim, Joo S., et al.** "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.
6. **Costigan Sean, Hennessy Michael** (2016): Cybersecurity: A Generic Reference Curriculum: NATO: ISBN 978-9284501960


*Сдана/Հանձնվել է՝ 22.05.2023*
*Рецензирована/Գրախոսվել է՝ 31.05.2023*
*Принята/Ընդունվել է՝ 07.06.2023*