ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 3 / UIF:8.2 / MODERNSCIENCE.UZ

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ В ЮРИДИЧЕСКИХ ФИРМАХ

Балтабаева Озода

Атаханова Фотимахон

Бекмуродов Дилшодбек

Мирзарахимов Хусан

https://doi.org/10.5281/zenodo.15104002

Аннотация. *В статье «Кибербезопасность и защита данных в юридических фирмах» исследуется проблематика защиты данных от различных кибератак в юридической сфере, анализируются ключевые угрозы и риски, а также мероприятия, которые необходимы для охраны конфиденциальности, целостности и доступности данных, представляется всесторонний анализ международного опыта в данной реалии. В этом исследовании акцентируется значимость создания политики безопасности, контроля за доступом, обучения сотрудников и соблюдения действующих законодательных норм. Гарантия безопасности информации в сфере юриспруденции является жизненно важной задачей, требующей постоянного мониторинга и адаптации.*

Ключевые слова: *кибербезопасность, конфиденциальность, персональные данные, киберпреступность, кибератаки, юридическая деятельность, юридические фирмы, защита данных, антивирус, фишинг, VPN, киберпреступления.*

CYBERSECURITY AND DATA PROTECTION IN LAW FIRMS

Abstract. *The article "Cybersecurity and data protection in law firms" examines the problems of data protection from various cyberattacks in the legal field, analyzes key threats and risks, as well as measures that are necessary to protect the confidentiality, integrity and availability of data, and presents a comprehensive analysis of international experience in this reality. This study emphasizes the importance of creating a security policy, access control, employee training and compliance with applicable laws. Ensuring information security in the field of jurisprudence is a vital task that requires constant monitoring and adaptation.*

Keywords: *cybersecurity, confidentiality, personal data, cybercrime, cyberattacks, legal activity, law firms, data protection, antivirus, phishing, VPN, cybercrime.*

Цель исследования: изучить проблематику кибербезопасности и защиты данных в юридических фирмах и организациях, дать рекомендации по улучшению обеспечения

кибербезопасности. Для достижения поставленной цели будут поставлены нижеследующие задачи:

1. Изучение понятий кибербезопасность и защита данных.
2. Рассмотрение кибербезопасности в рамках юридической практики.
3. Изучение проблемы кибератак
4. Анализ международного опыта
5. Рекомендации по улучшению обеспечения кибербезопасности в юридических фирмах.
6. Законодательство Республики Узбекистан

МЕТОДЫ

Данное исследование было проведено с использованием различных методов изучения. Использовались следующие методы:

Анализ литературы: Теоретические основы темы были изучены путем анализа научных статей и книг по данному направлению. В процессе анализа осуществлялся поиск с помощью ключевых слов, таких как: «кибербезопасность», «защита данных в юридических фирмах», «кибератаки и ее основные виды»

Контент анализ: обзор вебсайтов юридических фирм с рекомендациями по обеспечению кибербезопасности в организации.

ВВЕДЕНИЕ

В последние годы технологические инновации нашли свое отражение и в сфере юриспруденции. Вместе с развитием технологий и цифрового мира, развиваются и новые пространства для правонарушений и преступлений. Потому в наше время высококвалифицированному юристу важно иметь не только интеллектуальное лидерство, но и навыки использования технологий в юридической практике. (Legal Tech)

Юридические организации обрабатывают и хранят большое количество конфиденциальной информации, включая персональные данные своих клиентов, судебные документы, договоры, финансовые данные и др. Вопрос кибербезопасности актуален не только в контексте защиты данных оппонента, но и в целом секретной информации государства. В данной статье будут рассмотрена проблематика защиты данных в юридических организациях, основные угрозы и риски кибератак, а также предложены рекомендации по обеспечению кибербезопасности.

1.1 Кибербезопасность представляет собой практику, направленную на защиту компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных кибератак. Это явление также известно под терминами «безопасность информационных технологий» или «безопасность электронной информации». Реализация действенных мер киберзащиты становится особенно трудной задачей в нынешнее время, когда количество устройств превышает численность пользователей, а киберпреступники становятся все более изобретательными и инновационными. Эффективная стратегия кибербезопасности подразумевает наличие многоуровневой защиты для компьютеров, сетей, программ и данных, которые пользователь стремится сохранить в безопасности. В рамках организации единой системы управления угрозами возможно автоматизировать взаимодействие между различными продуктами, что ускоряет ключевые аспекты безопасности: обнаружение, расследование и устранение угроз. Люди, процессы и технологии должны гармонично дополнять друг друга, чтобы сформировать мощную защиту от кибератак.

1.2 Защита данных — это процесс защиты важных данных от повреждения, компрометации или потери и предоставления возможности восстановить данные до функционального состояния, если что-то произойдет, что сделает данные недоступными или непригодными для использования. Защита данных гарантирует, что данные не будут повреждены, доступны только для разрешенных целей и соответствуют применимым законодательным или нормативным требованиям. Защищенные данные должны быть доступны при необходимости и пригодны для использования по назначению.

2. Кибербезопасность в юридических фирмах.

Учитывая, что юридические фирмы обрабатывают конфиденциальные данные клиентов на нескольких уровнях, их системы безопасности должны быть усилены в геометрической прогрессии. Фирмы должны пересмотреть свои системы безопасности и установить строгие протоколы безопасности, чтобы обеспечить защиту данных клиентов и конфиденциальность.

3.1 Кибератаки

Кибератака — это любая преднамеренная попытка украсть, раскрыть, изменить, отключить или уничтожить данные, приложения или другие активы посредством несанкционированного доступа к сети, компьютерной системе или цифровому устройству.

Мотивы кибератак могут быть разными, но можно выделить три основные категории:

1. Криминальный
2. Политический
3. Личностный

Преступники, **криминально мотивированные,** стремятся получить финансовую выгоду посредством кражи денег, кражи данных или нарушения работы бизнеса. Киберпреступники могут взломать банковский счет, чтобы украсть деньги напрямую, или использовать мошенничество с социальной инженерией, чтобы обманом заставить людей отправить им деньги. Хакеры могут украсть данные и использовать их для совершения кражи личных данных или продать их в даркнете или удерживать их с целью получения выкупа.

Вымогательство — еще одна используемая тактика. Хакеры могут использовать программы-вымогатели, DDoS-атаки или другие тактики, чтобы удерживать данные или устройства в заложниках, пока компания не заплатит. Однако, согласно последнему индексу угроз X-Force , 32 процента киберинцидентов были связаны с кражей и продажей данных, а не с шифрованием для вымогательства.

Лично мотивированные злоумышленники, такие как недовольные нынешние или бывшие сотрудники, в первую очередь ищут возмездия за какое-то предполагаемое пренебрежение. Они могут отобрать деньги, украсть конфиденциальные данные или нарушить работу систем компании.

Политически мотивированные нападающие часто связаны с кибервойной, кибертерроризмом или «хактивизмом». В кибервойне субъекты национальных государств часто нацеливаются на правительственные учреждения или критически важную инфраструктуру своих врагов. Например, с начала российско-украинской войны обе страны столкнулись с серией кибератак на жизненно важные учреждения. Активисты-хакеры, называемые «хактивистами», могут не нанести значительного ущерба своим целям. Вместо этого они обычно привлекают внимание к своим целям, делая свои атаки известными общественности.

3.2 Наиболее распространенные виды кибератак.

Malware – (вредоносное ПО это термин, используемый для описания вредоносного ПО, включая шпионское ПО, ПО-вымогателя, вирусы и червей. Вредоносное ПО проникает

в сеть через уязвимость, как правило, когда пользователь нажимает на опасную ссылку или вложение электронной почты, которое затем устанавливает опасное ПО. Попав в систему, вредоносное ПО может сделать следующее:

•Блокирует доступ к ключевым компонентам сети (программы-вымогатели)

•Устанавливает вредоносное ПО или дополнительное вредоносное программное обеспечение

•Скрыто получает информацию, передавая данные с жесткого диска (шпионское ПО)

•Нарушает работу определенных компонентов и делает систему неработоспособной

Фишинг - это практика отправки мошеннических сообщений, которые, как представляется, исходят из надежного источника, обычно по электронной почте. Цель — украсть конфиденциальные данные, такие как данные кредитной карты и входа в систему, или установить вредоносное ПО на компьютер жертвы. Фишинг становится все более распространенной киберугрозой.

Spoofing- (подмена) киберпреступники иногда подражают людям или компаниям, чтобы обманом заставить вас раскрыть личную информацию. Это может произойти по-разному. Распространенная стратегия спуфинга предполагает использование поддельного идентификатора вызывающего абонента, при котором человек, принимающий вызов, не видит, что номер фальсифицирован. Другие методы подделки включают в себя подрыв систем распознавания лиц, использование поддельного доменного имени или создание поддельного веб-сайта.

4.1 Международный опыт.

Для стран как с низким, так и с высоким уровнем риска кибербезопасность является критической линией обороны. Однако некоторые страны лидируют в законодательстве о кибербезопасности, торговле, национальных стратегиях и защите критической инфраструктуры. Их доступ к квалифицированным экспертам в этом секторе, несомненно, способствовал их развитию. Компания по разработке программного обеспечения для предотвращения мошенничества Seon извлекла данные из индекса глобальных киберстратегий и недавней статистики киберпреступности, чтобы определить, какие страны лидируют в этой области. Согласно рейтингу кибербезопасности по странам, это три самые безопасные страны в порядке их рейтинга:

1. **Дания.** Дания, получившая рейтинг самой безопасной в цифровом отношении страны в мире, набрала 8,91.

2. **Германия.** Благодаря всеобъемлющим законам и правилам Германия набрала 8,76 балла в рейтинге Seon.

3. **Соединенные Штаты.** У США сильное законодательство и низкая подверженность киберпреступлениям, что принесло им третье место и оценку 8,72.

Также стоит отметить, Глобальный индекс кибербезопасности ITU ставит Саудовскую Аравию на четвертое место наряду с Великобританией. По словам Шилпи Ханды, заместителя директора по исследованиям МСЭ, Саудовская Аравия «добилась значительных успехов в укреплении своей инфраструктуры кибербезопасности». В прошлом году Королевство потратило 1,2 миллиарда долларов на обучение молодых людей кибербезопасности, чтобы не отставать от будущих угроз.

Понимание того, как определяются эти рейтинги, может выделить критические области в подходе страны к кибербезопасности.

Центр Белфера по международным научным вопросам в Гарвардской школе Кеннеди выпускает национальный отчет Cyber Power Index, в котором страны ранжируются по уровню кибермощи. Кроме того, в отчете определяются национальные цели, которые необходимо разработать странам для повышения уровня своей кибербезопасности. Цели включают внешнюю разведку, наблюдение и мониторинг внутренних групп и укрепление национальной кибероборонь.

Кроме того, IT-компания Comparitech также ранжирует страны по уровню их кибербезопасности. Они отмечают количество хакерских атак, вредоносных программ, криптомайнинга и фишинговых атак, а также связи между социальными сетями и кибербезопасностью как часть своих расчетов.

5.1 Рекомендации по защите от кибератак и улучшению обеспечения кибербезопасности в юридических фирмах.

Предотвращение инцидентов кибербезопасности заключается не только в наличии технологической защиты, но и в принятии поведения, которое может ограничить глубину и широту атаки. На самом деле, как ни удивительно для некоторых, предотвращение атак больше не является реалистичной целью для юридических фирм. Сегодня это вопрос максимально быстрого и эффективного реагирования на неизбежную атаку. «Киберпреступность впервые обгоняет все другие формы преступлений, поэтому

потребность в защите определенно есть», — сказал Дэвис Кесслер, руководитель отдела киберрисков в Travelers Europe. «Если компания, хранящая информацию об индивидуальных или корпоративных клиентах, подвергнется взлому — с помощью вредоносного ПО, фишинговых схем или множества других способов, — компания будет нести ответственность».

Рекомендации по защите данных и кибербезопасности представлены ниже:

•Межсетевые экраны сетевой безопасност

•Антивирусное программное обеспечение.

• Виртуальные частные сети (VPN)

Конфиденциальное общение является краеугольным камнем юридической профессии. Юридические фирмы должны использовать защищенные системы электронной почты и платформы обмена сообщениями. Также, где это уместно, виртуальные частные сети (VPN) для обеспечения конфиденциальности клиентских коммуникаций и защиты от перехвата.

• Многофакторная аутентификация (МИД)

Многофакторная аутентификация добавляет дополнительный уровень безопасности учетным записям пользователей. Требуя вторую форму проверки (например, код, отправленный на мобильный телефон) в дополнение к паролю, юридические фирмы могут снизить риск несанкционированного доступа к электронным письмам и записям.

• Шифрование данных

•Решения для обеспечения безопасности конечных точек.

•Проведение регулярных программ обучения и повышения осведомленности сотрудников.

Человеческая ошибка является одной из основных причин нарушений кибербезопасности. Обучение персонала распознаванию попыток фишинга, использованию надежных паролей и соблюдению протоколов защиты данных имеет важное значение. Постоянные программы повышения осведомленности о кибербезопасности могут значительно снизить риск человеческой ошибки.

6.1 Законодательство Республики Узбекистан

Данная сфера регулируется следующими нормативно правовыми актами:

Закон Республики Узбекистан «О кибербезопасности», принятый 25 февраля 2022 года, регулирует отношения в сфере кибербезопасности. Закон Республики Узбекистан «Об

электронном Правительстве» был принят 18 ноября 2015 года, регулирует отношения в сфере электронного правительства. Закон Республики Узбекистан «О персональных данных»

ЗАКЛЮЧЕНИЕ

Кибербезопасность больше не является просто вопросом ИТ — это критически важная для бизнеса проблема юридических фирм. Риски, связанные с кибератакой, могут быть разрушительными, влияя не только на деятельность фирмы, но и на ее репутацию и доверие клиентов. Инвестируя в надежные меры кибербезопасности, соблюдая нормативные требования и развивая культуру осведомленности, юридические фирмы могут защитить своих клиентов и свой бизнес от этой растущей угрозы. Таким образом, вопрос обеспечения информационной безопасности в юридической сфере остается открытым и имеет ряд вопроров, которые необходимо решать на уровне государства, необходимо формирование нормативно-правовой базы, рекомендаций и методических пособий для юристов по работе с конфиденциальной информацией. Крометого необходимо реализовать программы обучения по формированию навыков и умений по работе с конфиденциальной юридической информацией. Реализация данных мероприятий позволит решить ряд проблем по обеспечению информационной безопасности в юридической сфере.

REFERENCES

1. https://cyberleninka.ru/article/n/zaschita-informatsii-v-yuridicheskoy-deyatelnosti/viewer
2. https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity-law-firms/
3. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
4. https://www.ibm.com/topics/cyber-attack#Why+do+cyberattacks+happen%3F%C2%A0
5. https://lawware.co.uk/blog/law-firm-cyber-attacks/
6. https://www.travelers.co.uk/industry-solutions/legal-sector/how-to-help-protect-your-law-firm
7. https://cyberleninka.ru/article/n/problemy-zaschity-informatsii-v-yuridicheskoy-sfere/viewer
8. https://www.igi-global.com/chapter/cyber-security-strategies/332286
9. https://www.mimecast.com/content/cybersecurity-for-law-firms/