ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ
МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
INTERNATIONAL UNIVERSITY

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2023 (15) 3

Шілде – қыркүйек

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

---

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

МАЗМҰНЫ

ӘЛЕУМЕТТІК-ЭКОНОМИКАЛЫҚ ЖҮЙЕЛЕРДІ ДАМЫТУДАҒЫ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

СОДЕРЖАНИЕ

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ СОЦИО-ЭКОНОМИЧЕСКИХ СИСТЕМ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

CONTENTS

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 4. Is. 3. Number 15 (2023). Pp. 59–67
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2023.15.3.005

УДК 004.5

RISKS AND THREATS IN THE FINANCIAL SECTOR OF KAZAKHSTAN

L.M. Alimzhanova[1]*, E.M. Panova[1], Bohdan Haidabrus[2]

Laura M. Alimzhanova — Cand. Sc. (Technology), Associate Professor of the Department of «Information Systems» of the International Information Technology University, Almaty
Yerkezhan M. Spanova — master student, International Information Technology University, Almaty
Bohdan Haidabrus — PhD, Cand.of Tech.Science. Riga Technical University, Riga, Latvia
https://orcid.org/0000-0002-9040-9058

Abstract. The article discusses possible threats and risks for the country's financial institutions associated with information leakage. Various measures are proposed to reduce and neutralize such risks and increase the awareness of employees in the basics of cybersecurity. Since every year potential threats grow, it is necessary to ensure the security of financial institutions. For the functioning of the company, these risks are the probability of the worst scenario, and the threat can negatively affect the scenario from the outside. These risks negatively impact the company's ability to operate properly and generate financial returns. In some cases, risks can even lead to the bankruptcy of the company. Therefore, identifying these risks allows companies to prepare their organizational structures for various types of threats and minimize the impact of adverse events. It is a standard procedure and a key element of business planning. In addition, the article describes the most used cyber-attacks, company security methods and a financial analysis of cybersecurity in general.

Keywords: financial r isks, cybersecurity, i nformation s ecurity policy, l eakage of confidential information, software, threat neutralization, social engineering

For citation: L.M. Alimzhanova, E.M. Panova, Bohdan Haidabrus. Risks and threats in the financial sector of kazakhstan//INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2023. Vol.4. No.3. Pp.59–67 (In Russ.). https://doi.org/10.54309/IJICT.2023.15.3.005

ҚАЗАҚСТАННЫҢ ҚАРЖЫ САЛАСЫНДАҒЫ ТӘУЕКЕЛДЕР МЕН ҚАТЕРЛЕР

Л.М. Әлімжанова[1]*, Е.М. Спанова[1], Bohdan Haidabrus[2]

Әлімжанова Лаура Мұратбекқызы — т.ғ.к., Халықаралық ақпараттық технологиялар университетінің "Ақпараттық жүйелер" кафедрасының қауымдастырылған профессоры
Спанова Еркежан Магбатқызы — халықаралық ақпараттық технологиялар университетінің магистранты
Bohdan Haidabrus — PhD. тех. Канд.Ғылым Рига Техникалық Университеті, Рига, Латвия
https://orcid.org/0000-0002-9040-9058

Аннотация. Аңдатпада ақпараттың ағып кетуіне байланысты елдің қаржы институттары үшін ықтимал қауіптер мен тәуекелдер талқыланады. Мұндай тәуекелдерді азайту және бейтараптандыру және қызметкерлердің киберқауіпсіздік негіздерінен хабардарлығын арттыру үшін әртүрлі шаралар ұсынылады. Жыл сайын әлеуетті қауіптер артып отырғандықтан, қаржы институттарының қауіпсіздігін қамтамасыз ету қажет. Компанияның жұмыс істеуі үшін бұл тәуекелдер ең нашар сценарийдің ықтималдығы болып табылады, ал қауіп - бұл сценарийге сырттан теріс әсер етуі мүмкін барлық нәрсе. Бұл тәуекелдер компанияның дұрыс жұмыс істеу және қаржылық кіріс алу қабілетіне теріс әсер етеді. Кейбір жағдайларда тәуекелдер тіпті компанияның банкрот болуына әкелуі мүмкін. Сондықтан бұл тәуекелдерді анықтау компанияларға өздерінің ұйымдық құрылымдарын қауіптердің әртүрлі түрлеріне дайындауға және жағымсыз оқиғалардың әсерін барынша азайтуға мүмкіндік береді. Бұл стандартты процедура және бизнес-жоспарлаудың негізгі элементі. Сонымен қатар, мақалада ең жиі қолданылатын кибершабуылдар сипатталған; компанияның қауіпсіздік әдістері; жалпы киберқауіпсіздікке қаржылық талдау жүргізді.

Түйін сөздер: қаржы тәуекелі, ақпараттық қауіпсіздік, ақпараттық қауіпсіздік саясаты, ақпараттың жайылып кетуі, бағдарламалық жасақтама, қатерлерді бейтараптандыру, әлеуметтік инженерия

Дәйексөз үшін: Л.М. Әлімжанова, Е.М. Спанова, Bohdan Haidabrus. Қазақстанның қаржы саласындағы тәуекелдер мен қатерлер//Ақпараттық және коммуникациялық технологиялардың халықаралық журналы. 2023. V.4. № 3. Бет 59–67 (ағылшын тілінде). https://doi.org/10.54309/IJICT.2023.15.3.005

РИСКИ И УГРОЗЫ В ФИНАНСОВОЙ СФЕРЕ КАЗАХСТАНА

Л.М. Алимжанова[1]*, Е.М. Спанова[1], Bohdan Haidabrus[2]

Алимжанова Лаура Муратбековна — к.т.н., ассоциированный профессор кафедры «Информационные системы» Международного университета информационных технологий
Спанова Еркежан Магбаткызы — магистрант Международного университета информационных технологий
Bohdan Haidabrus — Кандидат технических наук, Рижский технический университет, Рига, Латвия

Аннотация. В статье рассматриваются возможные угрозы и риски для финансовых институтов страны, связанных с утечкой информации. Предлагаются различные меры для уменьшения и нейтрализации таких рисков и повышения грамотности сотрудников в основах кибербезопасности. Так как с каждым годом потенциальные угрозы и риски увеличиваются, необходимо обеспечивать безопасность финансовых учреждений на должном уровне. Для функционирования компании данные риски — это вероятность худшего сценария, а угроза — это все, что может негативно повлиять на сценарий извне. Эти риски негативно влияют на способность компании работать должным образом и получать финансовую прибыль. В отдельных случаях риски могут привести к банкротству компании. Поэтому, выявление таких рисков позволяет компаниям подготовить свои организационные структуры к различного рода угрозам и минимизировать влияние неблагоприятных событий. Это стандартная процедура и ключевой элемент бизнес-планирования. Кроме этого, в статье описываются наиболее часто используемые кибератаки, методы обеспечения безопасности компании и проводится финансовый анализ кибербезопасности в целом.

Ключевые слова: финансовые риски, кибербезопасность, политика информационной безопасности, утечка конфиденциальной информации, программное обеспечение, нейтрализация угроз, социальная инженерия

Для цитирования: Л.М. Алимжанова, Е.М. Спанова, Bohdan Haidabrus. Риски и угрозы в финансовой сфере казахстана//Международный журнал информационных и коммуникационных технологий. 2023. Т. 04. № 3. Стр. 59–67 (На анг.). https://doi. org/10.54309/IJICT.2023.15.3.005

Введение

Функционирование и развитие каждого государства сопряжено со множеством рисков и осуществляется в условиях нарастающих кризисов. Их последствия дестабилизируют многие системы и представляют глобальные угрозы для безопасности. В первую очередь, это касается экономической системы. И в ситуации непрерывных потенциально деструктивных изменений каждая структура, организация, компания постоянно соприкасаются с существующими рисками в текущих условиях.

В данное время одним из самым распространённых рисков считается риск нарушения конфиденциальности информации, а именно утечка конфиденциальных данных. Она может произойти по ряду причин: взлом и проникновение в структуру компании третьего лица, несанкционированное скачивание сотрудником нелегитимного программного обеспечения (ПО), который содержит вирус, промышленный шпионаж, человеческий фактор и т.д.

С каждым годом кибербезопасность становится все более важным фактором системы безопасности для предприятий, компаний и фирм любого размера практически во всех отраслях экономики. В 2020 году случаи программ-вымогателей выросли на 150 %, и каждые 39 секунд где-то в сети запускается новая атака. Так, в январе 2021 года в Казахстане было совершено более 3 тыс.

кибератак — в 2,8 раза больше по сравнению с январем предыдущего года. При этом годом ранее количество кибератак показывало спад на 30,5 %. Такие данные в разное время публиковал сайт ranking.kz.

Согласно международным экспертным данным, финансовые, материальные, имущественные, экономические и др. ущербы возрастают ежегодно, что связано с увеличением кибератак. На данный момент мировым экспертным сообществом прогнозируемая сумма планетарного ущерба составляет до 8 трлн доларов (https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/).

Чаще всего утечка данных затрагивает финансово-банковскую сферу и вызывает в ней колоссальный рост расходов. Банки, финансовые организации — это та сфера, где находятся финансовые и денежные ресурсы, и именно поэтому финансовые учреждения зачастую являются главными объектами кибератак на разных уровнях. Киберпреступления содержат множество способов получения доходов за счет вымогательства, краж и мошенничества. И параллельно подобные преступления совершают не только хактивисты, но и даже государства, которые нацелены на финансовый сектор для политического, идеологического и информационного воздействия и влияния. Органы управления, являясь регуляторами этой сферы, постоянно обращают на это внимание и активизируют разработку и внедрение новых средств контроля кибер-рисков, чтобы противостоять растущим угрозам, ослабляющим национальную безопасность, экономику и др.

Цель статьи - рассмотрение рисков, способов нейтрализации угроз и методов защиты в ситуациях утечки информации.

Предметом данного исследования являются риски, которые связаны с утечкой информации.

Объектом данного исследования является финансовая сфера.

Задачи статьи:

- описать репутационные и операционные риски;
- рассмотреть кибератаки в финансовой индустрии;
- расписать методы обеспечения безопасности на корпоративном уровне
- провести финансовый анализ кибербезопасности в финансовых учреждениях

Финансовые риски

Традиционно в финансовой сфере основные риски делятся на несколько групп. Остановимся на двух основных из них:

репутационные (имиджевые) риски;

операционные риски.

Репутационный риск

Управление репутационными рисками в финансовых учреждениях является одной из наиболее ценных стратегий для финансовой организации. Управление репутацией является базой любой компании, стремящейся к эффективной деятельности и долгосрочному развитию. Солидная репутация — это высокие показатели работы, повышенный спрос на продукцию товаров и услуг, это растущая клиентская база и др. В то же время негативная репутация может оттолкнуть потенциальных клиентов и увеличить их отток, что в условиях высокой

конкуренции может привести не только к снижению доходов, потери прибыли, но и к банкротству. Мониторинг отзывов клиентов, проводимый многими компаниями, показывает, что происходит снижение доверия к финансовым структурам, которые все чаще занимают предпоследнее место в рейтинге репутации по сравнению с другими отраслями.

В отношении кибербезопасности можно сказать, что в настоящий момент она является основной составляющей репутации компании. И наиболее уязвимыми сейчас являются платежные порталы, представляющие повышенный интерес для преступников. Это значительный риск для безопасности компаний и их клиентов. Вторым по значимости риском является компрометация данных для входа в систему. Многие пользователи и потребители используют один и тот же пароль для всех своих платформ, поэтому взлом одной из них означает угрозу для всех.

Поскольку крупные корпорации тщательно защищают свои собственные и управляемые активы, риски существенны и для собственных, и для сторонних пользователей (партнеров, поставщиков, дочерних компаний и др.). К примеру, небольшие предприятия редко имеют одинаковые протоколы безопасности, но могут хранить или иметь доступ к данным клиента. Самый простой пример утечки данных, влияющей на репутацию — утечка данных Target в 2013 году. Продажи резко упали после взлома стороннего поставщика, повлекшего за собой раскрытие 40 миллионов кредитных и дебетовых карт по всему миру. Впоследствии компания Target была вынуждена уволить тысячи корпоративных и розничных сотрудников и только недавно сумела частично восстановить репутацию и вернуть некоторое доверие.

Практика показывает, что после раскрытия информации о взломе цены на акции падают минимум на пять процентов. Тем не менее, акции могут восстанавливать свою стоимость, если компания сразу же в течение нескольких дней открыто сообщает о нарушениях/взломах/утечках, тем самым не только стабилизируя ситуацию, но и повышая свою репутацию как в области обеспечения безопасности, так и в целом репутацию бренда. Кроме этого, такие механизмы взаимодействия с клиентами повышают уровень их лояльности.

Операционный риск

Операционный риск определяется как возможность убытков в результате сбоя внутренних процессов/систем/внешних событий и др. Сюда же относится и человеческий фактор. Выделяются следующие виды операционных рисков:

- фидуциарные нарушения;
- агрессивные продажи;
- нарушения конфиденциальности;
- отказ ИТ-систем;
- судебные разбирательства;
- неправомерное использование конфиденциальной информации и др.

Организация контролирует операционные риски посредством оценки реальных и потенциальных угроз, выработки методов повышения безопасности, усиления управления рисками, включая внешние и внутренние факторы. К

внешним факторам могут относиться стихийные бедствия, политический фактор, дестабилизация финансовой системы, внешнее вмешательство (в том числе правонарушения, киберпреступления, мошенничество и др.). К внутренним факторам относятся технические сбои существующих систем, неэффективное обслуживание оборудования и серверов, нерегламентируемые технические и организационные процессы.

Одной из наиболее распространенных угроз в современном цифровом мире является возможность использования DDOS-атак. Это распространенный метод прерывания бизнес-операций, представляющий собой интенсивную атаку на сервер целевой фирмы. Например, несколько лет назад в Казахстане серверы нескольких банков подверглись DDoS-атакам. По информации «Интерфакса» в период с 26 по 29 сентября 2017 года хакеры использовали ботнет из устройств, находящихся в более чем 50 странах (http://lib.itsec.ru/newstext.php?news_id=119080).

Кроме подобных угроз существуют и другие их виды. Наиболее распространенными являются мошенничество с идентификацией и картами, фишинговые электронные письма, скимминг и подделка карт. Последние являются основным видом мошенничества, связанных с использованием дебетовых карт. В случаях такого мошенничества преступники получают доступ к конфиденциальной информации, учетным данным клиентов, используют онлайн-платежи в корыстных целях, нанося огромный ущерб как финансовой структуре, потребителям финансовых услуг, клиента и др.

Кибератаки в финансовой индустрии

Ниже приведены наиболее распространенные типы атак, используемые против компаний, предоставляющих финансовые услуги, которые могут повлечь утечку конфиденциальных данных.

Атаки на веб-приложения. Многие организации полагаются на веб-приложения для своих бизнес-операций, причем Google Suite является одним из самых популярных. Эти приложения упрощают сотрудникам обмен файлами и совместную работу. Однако эти службы уязвимы для атак из-за простоты доступа и зависимости от действий пользователя. Эти типы атак могут привести к непроверенным перенаправлениям или ссылкам, которые обманным путем заставляют пользователей щелкнуть мышкой.

Боты: Боты — это, по сути, автоматизированные программы, предназначенные для выполнения задач в Интернете. Многие предприятия финансового сектора часто используют ботов. Они часто используются для улучшения обслуживания клиентов. Однако есть хорошие боты, а есть плохие боты. Вредоносный бот может быть запрограммирован на прямую или косвенную атаку на учреждение — например, его можно использовать для рассылки спама по электронной почте или для взлома паролей методом грубой силы.

Программа-вымогатель. Программа-вымогатель — это тип вредоносного ПО, которое после заражения системы может зашифровать ваши файлы или даже операционную систему (ОС). Это эффективно блокирует доступ к важным документам или самому устройству. Это называется программами-вымогателями,

потому что часто преступник, стоящий за атакой, не расшифровывает систему, пока не будет выплачен выкуп. Это стало одним из наиболее часто встречающихся типов атак на финансовые компании и одним из наиболее опасных.

Фишинг. Фишинговые атаки почти так же распространены, как и атаки программ-вымогателей. Эти атаки используют социальную инженерию, чтобы заставить сотрудников выполнить действие, позволяющее установить вредоносное ПО в вашей сети.

Защита от кибератак на корпоративном уровне

Наиболее распространенным методами обеспечения кибербезопасности являются следующие:

Обучение сотрудников для обнаружения фишинговых писем. Сегодня фишинг является основной социальной атакой на бизнес, на которую приходится более 75 процентов нарушений безопасности. Поскольку никакое решение для обеспечения кибербезопасности не может стопроцентно заблокировать подобные атаки, необходимо внедрять или усиливать существующее обучение по вопросам фишинга. Это важно для понимания этого процесса и обеспечения индивидуальной защиты от фишинговых атак, так как устранение их последствий — процесс длительный, сопряжен со значительными затратами и может поставить под угрозу всю сеть инфраструктуры. Поэтому важно, чтобы организация в плане защиты работала как единая команда, действующая по установленному регламенту. Кроме этого, должна быть налажена система регулярного оповещения об атаках (к примеру, та же массовая рассылка, информирование через доступные источники и т.д.).

Несмотря на то, что рекомендуется проводить структурированные ежегодные или полугодовые тренинги по повышению кибербезопасности, компании должны разработать программы курсов развития информированности сотрудников о фишинге «на лету», когда использование ссылки содержит и немедленную обратную связь. К таким продуктам относятся, к примеру, программы KASAP (Kaspersky Automated Security Awareness Platform), согласно которым можно проходить обучение, тестирование, а также помощь администратора данной системы, который может распространить легитимные фишинговые сообщения, повышающие киберграмотность.

Интеграция и обновление политики информационной безопасности.

Политика ИТ-безопасности имеет решающее значение для успеха любой организации и является основой всех, формирует способность организаций к эффективному реагированию на инциденты безопасности. Информационная безопасность опирается на разработанный документированный регламент, соблюдаются всеми членами компании/организации. В этом вопросе для финансовых организаций актуализируется значение таких процедур как парольная политика систем и пользователей, регламент почты и корпоративных средств, и сама политика информационной безопасности. Политики информационной безопасности должны быть актуализированы согласно утвержденному стандарту.

Постоянное уведомление сотрудников о новых атаках.

Статистика кибербезопасности по итогам прошлых пандемийных лет показывает огромный рост взломанных данных из источников, которые все чаще встречаются на рабочем месте (мобильные устройства и устройства IoT). Кроме этого, COVID-19 расширил возможности для кибератак через активное использование форм дистанционной работы (удаленка). В связи с этим необходимо повышать информирование сотрудников и о новых видах атак (посредством той же массовой рассылки, регулярных оповещений, постов в корпоративных сетях и др.).

Использование различного вида защитных IT-систем. По данным статистики в 2021 году количество кибератак увеличилось на 6,5 % по сравнению с 2020 г. (Статья: Число_кибератак_в_России_и_в_мире). Преступники все больше используют социальную инженерию, эксплуатируя недостатки защиты и уязвимости в ПО, а также применяя заведомо вредоносные ПО. В целях обеспечения безопасности системы необходимо использовать такие инструменты защиты, как антивирусы, DLP-системы, программы-«ловушки», разного рода SIEM и т.д.

Финансовый анализ кибербезопасности в финансовых учреждениях

Для обеспечения защиты всей инфраструктуры используются различного вида IT-системы. Данные системы должны покрывать на 100 % корпоративные сервера, ноутбуки, защищать и мониторить в режиме реального времени. Приоритетом каждой компании является защита сначала корпоративных ноутбуков, так как, согласно исследованиям, 90 % утечек данных происходит вследствие человеческого фактора, а не внешних действий хакеров. Для того, чтобы предотвратить утечку конфиденциальных данных, используются специальные технологии, а именно DLP-системы. Они могут анализировать и проводить экспертизу потока данных. Также с помощью таких систем можно блокировать подключения, просматривать истории, а также выявлять некомпетентных сотрудников, в том числе превышающих свои полномочия. Так в одной крупной компании в 2021 году была предотвращена утечка данных в конкурирующую компанию, когда сотрудники, используя переносное устройство, пытались отправить данные конкурентам.

Следующим не менее важным инструментом защиты является различного вида антивирусы, которые ставятся как на сервера, так и на устройства сотрудников. Они как минимум могут блокировать запуск нелегитимного ПО, удаленно обновлять политики самого устройства, а также мониторить действия пользователей. Антивирусы могут блокировать до 80 % кибератак на компанию. Самым главным преимуществом является постоянное автоматическое обновление.

Сетевые ловушки также успешно используются для защиты инфраструктуры. Они представляют собой приманку, которая помогает заблокировать действия злоумышленника. Такие ловушки часто называют honeypot. Самым главным сильным фактором данной системы является то, что сотрудники кибербезопасности могут не знать, что произошла кибератака и хакер проник во внутреннюю сеть компании. Однако благодаря заблаговременным выставленным ловушкам, которые могут имитировать сеть, сервер, или же другую систему, он не сможет дальше продолжать свои действия. Хоть они и не покрывают инфраструктуру на 100 %, но считается очень эффективными.

SIEM-системы как и антивирусы, DLP-системы могут обеспечивать анализ событий в реальном времени, однако они больше применяются для обеспечения целостности серверов. Они глубже проводят экспертизу, так можно узнать откуда была произведена кибератака.

В таблице 1 ниже представлены цены на вышеописанные IT-продукты:

Таблица 1. Цены на IT-продукты

Антивирусы	От 10 000 тг, 1 устройства
DLP-система	От 60 000 тг, 100 устройств
Сетевая ловушка	От 20 000 тг, 1 устройство
SIEM-система	От 20 000 000 тг
Примечание: составлено автором по открытом источникам	

Заключение

В ближайшее время в связи с повышением частоты кибератак, нейтрализация угроз и рисков финансовой сферы в рамках кибербезопасности выходит на первый план и предполагает создание системной безопасности на всех уровнях как исполнителей, так и руководства. Также требуется постоянный мониторинг рисков, который предполагает повышение уровня компьютерной грамотности сотрудников и персонала, через различные курсы повышения квалификации по кибербезопасности и необходимо ежегодные проверки аудита, соблюдения контроля согласно стандарту текущего года для эфектимвного управления информацией.

Появление новых технологий и шпионских программ требует постоянного обновления программного обеспечения и дополнительных финансовых и технических ресурсов.

ЛИТЕРАТУРА

https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/;

http://lib.itsec.ru/newstext.php?news_id=119080;

https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире;

https://www.reviewtrackers.com/blog/bank-reputation-risk-management/;

https://www.researchgate.net/publication/315038404_A_Study_of_Risk_Management_in_Finance_Sector

https://cyberleninka.ru/article/n/finansovye-riski-metody-otsenki-i-podhody-k-upravleniyu;

https://esj.today/23ecvn518.html;

https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/;

https://quickbooks.intuit.com/ca/resources/running-a-business/train-employees-recognize-phishing-emails/;

https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/financial-sector;

https://applied-research.ru/ru/article/view?id=7055;

https://kapital.kz/tehnology/93798/kolichestvo-kiberatak-v-kazakhstane-uvelichilos-pochti-v-3-raza.html.

Rene' M Stulz, "Risk Management and & Derivatives,,, 2003. RS Raghavan, Risk Management in Banks -ICAI publication, Feb 2013 (www. i cai.org/ reso urce_ file/ I I 49 Opga I -g5 1.pdf)

Verma S B, Risk management -Deep & Deep publications

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

ОТВЕТСТВЕННЫЙ РЕДАКТОР
Мрзабаева Раушан Жалиевна

КОМПЬЮТЕРНАЯ ВЕРСТКА
Жадыранова Гульнур Даутбековна

Подписано в печать 15.09.2023.
Формат 60x881/8. Бумага офсетная. Печать - ризограф.6,5 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59