1
НОМЕР

ISSN 2304-9081
ЭЛЕКТРОННЫЙ ЖУРНАЛ
On-line версия журнала на сайте
http://www.elmag.uran.ru

БОНЦ

БЮЛЛЕТЕНЬ

ОРЕНБУРГСКОГО НАУЧНОГО ЦЕНТРА УрО РАН

Lycosa singoriensis (Laxmann, 1770)
Тарантул южнорусский
Шовкун Д.Ф.

2019

УЧРЕДИТЕЛЬ
ОРЕНБУРГСКИЙ НАУЧНЫЙ ЦЕНТР УрО РАН

Б.И. Оспанов[1], А.М. Нурушева[2], М.Ж. Нурушев[2]

О НОВЫХ СОВМЕСТНЫХ МЕТОДАХ ЗАЩИТЫ ОТ КИБЕРАТАК В КАЗАХСТАНЕ

[1] Академия государственного управления при Президенте РК, Нурсултан, Казахстан
[2] Евразийский национальный университет им. Л.Н. Гумилева, Нурсултан, Казахстан

В обзоре рассмотрена значимость разработки отечественных программных продуктов, направленных на обеспечение надежности информационных систем, где необходимо принять к широкому внедрению разработки отечественных ученых для оценки рисков программных продуктов. Укреплять сотрудничество Казахстана со специалистами из РФ по консолидации взаимных усилий, технических и человеческих ресурсов в области защиты от кибератак. Необходима последовательность реализации информационной безопасности на основе государственной дорожной карты по кибербезопасности, где приоритетное место должно быть уделено подготовке кадров. Анализ обеспечения безопасности АС использующих стандарты серии ИСО/МЭК15408 показал надежность автоматических систем на основе снижения уровня рисков, методом уменьшения неприемлемых рисков до приемлемого уровня на основе периодической переоценки рисков и способности противостоять этим рискам.

Ключевые слова: киберугрозы, кибербезопасность, кибератаки, надежность, безопасность, показатели безопасности, оценка рисков.

B.I. Ospanov, A.M. Nurusheva, M.Zh. Nuryshev

ABOUT NEW JOINT METHODS OF PROTECTION FROM CYBERATAK IN KAZAKHSTAN

[1] Academy of Public Administration under the President of the Republic of Kazakhstan, Nursultan, Kazakhstan
[2] L.N. Gumilyov Eurasian National University, Nursultan, Kazakhstan

The paper is designed to analyze the methods and technologies of ensuring the functioning of information systems. The chain of introduction of information security should be based on the roadmap of the state cyber security, with priority of training (bachelors, masters, doctoral students) due to lack of qualified specialists in this area. It is necessary to open the institutes of professional development in the field of training of qualified personnel in accordance with international standards in the field of safety.

Key words: cyber threats, cyber security, cyber attacks, reliability, security, security metrics, risk assessment.

Цивилизованный мир определил киберриски как основную опасность в стратегических направлениях, каковыми на ближайшие годы являются бизнес, банковская сфера, оборонная промышленность. Весь мир признал киберугрозы как одну из сложнейших проблем развития любой страны.

Республика Казахстан этой теме уделяет особенное внимание как в ре-

DOI: 10.24411/2304-9081-2019-11004

шениях правительства в разных секторах экономики, так и путем привлечения собственной космической системы связи, что позволило нашей республике не только поднять престиж на мировой арене, но и оказать огромное влияние на безопасность многих сфер деятельности внутри страны.

В рамках Концепции кибербезопасности («Киберщит Казахстан»), утвержденной постановлением Правительства Республики Казахстан от 30 июня 2017 г. № 407, предлагаемая Стратегия определяет основные направления построения системы обеспечения кибербезопасности, включая эффективную защиту электронных информационных ресурсов, информационных систем, сетей телекоммуникаций субъектов финансового рынка, что позволит оперативно реагировать на существующие и вновь появляющиеся угрозы в киберпространстве. Следование данной Стратегии поможет достижению целей, сформулированных в Концепции.

Одним из первых в реализацию Стратегии включился Национальный Банк РК, планомерная деятельность которого была направлена на создание эффективной системы обеспечения кибербезопасности финансового сектора. Так, для достижения поставленной цели, с учетом отдельных текущих недостатков в части кибербезопасности финансового сектора, Национальный Банк определил пять основных направлений:

- совершенствование регулирования систем обеспечения кибербезопасности субъектов финансового сектора;
- обеспечение кибербезопасности физических и юридических лиц при использовании финансовых услуг;
- обеспечение устойчивого и безопасного функционирования критичной информационной инфраструктуры финансового сектора, включая Национальный Банк;
- сотрудничество в сфере борьбы с киберпреступностью в национальном и глобальном масштабе;
- создание и развитие национальных технологий киберзащиты финансового сектора.

Вместе с тем, следует отметить и надо признать, что основными рисками успешной реализации Стратегии кибербезопасности РК являются:

- недостаточность финансовых, материальных и интеллектуальных ресурсов в обеспечении планирования и реализации обязательных направлений Стратегии, а также внешние факторы, влияющие на доступность необходи-

DOI: 10.24411/2304-9081-2019-11004

мых ресурсов;

- слабое вовлечение первых руководителей организаций; отсутствие необходимой поддержки высшего руководства при реализации определенных в Стратегии задач;

- отсутствие консенсуса и компетенции в вопросах регулирования кибербезопасности; отличие подходов к определению необходимых мер и средств обеспечения кибербезопасности на государственном и отраслевом уровнях;

- отсутствие нормативно-правовой базы в области кибербезопасности на национальном уровне; устаревшая нормативно-правовая база, не адаптированная к существующим современным технологиям и преступлениям с их использованием.

Учитывая сложившиеся обстоятельства, надо осуществлять меры защиты как на международном уровне, кооперируясь с соседними странами, так и на внутригосударственном уровне централизованно (стандартно), чтобы сэкономить средства для этой цели. При этом крайне необходимы превентивные меры борьбы – для начала необходимо перекрыть основные пути доступа к информации для киберпреступников. На наш взгляд, таких методов всего два.

Первый – прежде всего, необходимо нейтрализовать вирусные угрозы, то есть обеспечить безопасность от проникновения опасных вирусных программ киберпреступников через программное обеспечение (ПО). Поэтому, хотя и крайне сложно, но необходимо проверить разработчиков софта на соответствие требованиям безопасности. Эту операцию можно осуществить на стадии лицензирования их продукции перед использованием на нашем рынке. Казахстан может выставить ряд необходимых требований всему перечню производителей ПО, а также участникам финансового сектора, подведомственного Нацбанку, обеспечить надежный контроль и мониторинг на соответствие безопасности. Только эффективный мониторинг поможет финансовым организациям удерживать риски кибербезопасности на необходимом уровне, своевременно совершенствовать и устранять недостатки существующих механизмов контроля. Проведение проверок финансовых организаций, сравнительный анализ результатов таких проверок, совместные учения с государственными органами и другие механизмы контроля позволят лучше понимать существующие киберугрозы и уязвимости в масштабе всего финансового сектора.

DOI: 10.24411/2304-9081-2019-11004

Второй – это нивелирование человеческого фактора, точнее говоря, устранение слабой компетентности сотрудников компаний в отношении видов киберрисков и методов их предотвращения. Мы хорошо знаем, когда пользователь, желая «сэкономить», приобретает нелицензированное программное обеспечение или скачивают его без оплаты, он попадает на «крючок» мошенников. Часто после активации такого ПО частным пользователям и компаниям приходит сообщение – для получения доступа к компьютеру, необходимо перевести некоторую сумму денег. При этом возможна утечка личных и корпоративных данных, они перестают быть секретом. Таких примеров можно привести множество. Безусловно, в рыночных условиях каждая компания самостоятельно несет ответственность за деятельность своего персонала, но данная проблема имеет большие масштабы в нашей стране, приобретая уровень национальной. Возникает вопрос, как обеспечить ликвидацию кибербезграмотности основной части пользователей ПО, в том числе не только в крупных компаниях, но и в малом, и среднем бизнесе.

Понимая всю сложность и ответственность указанной проблемы, в ее решении необходим комплексный подход на уровне государства – требуется всеобуч пользователей ПК основам кибербезопасности на государственной безвозмездной основе. Иными словами, вникая в масштабы опасности киберрисков и киберпреступности, необходимо, на основе методов ведущих стран мира стремиться к предупреждению кибератак, чем к ликвидации их последствий. Многие страны прекрасно усвоили, что превентивные мероприятия обходятся гораздо дешевле, чем «восстановительные работы».

Территория Республики Казахстан имеет свои особенности – огромная площадь с низкой плотностью населения, разнообразные рельефы местности, резко континентальный климат обусловили трудную задачу по обеспечению равных возможностей для всех граждан и всех секторов экономики вне зависимости от места их нахождения в решении вопросов доступа к инфокоммуникационным услугам и удовлетворении потребностей в телекоммуникациях. Следует отметить, что создание собственной космической системы связи позволило Казахстану оказать огромное влияние на различные сферы деятельности внутри страны. Наличие собственной космической системы связи – это защита национальных интересов, в том числе интересов обороны и государства в вопросах информационной безопасности, что является крайне актуальным в условиях нестабильности современных глобальных со-

DOI: 10.24411/2304-9081-2019-11004

циально-экономических вызовов в мире.

Анализируя возложенные задачи по обеспечению информационной безопасности, сохранности информационных ресурсов нашего государства, роль космической спутниковой связи (КСС) «KazSat» становится неоценимой. С другой стороны, собственная космическая система связи – это развитие сегментов отечественной экономики, а именно осуществление импортозамещения услуг по аренде спутниковой ёмкости у иностранных поставщиков. В результате значительные финансовые средства за использование спутниковыми операторами ресурсов национальных телекоммуникационных космических аппаратов сохраняются внутри республики. Только за счет эксплуатации с использованием КСС «KazSat», удалось обеспечить импортозамещение услуг на сумму порядка 22,2 млрд. тенге. Указанная космическая система связи в Казахстане охватывает 7 000 земных станций спутниковой связи, обеспечивает 15 операторов связи и организаций республики, где работают более 200 постоянных специалистов высоких квалификации. И, наконец, собственная космическая система связи – это ликвидация в стране «цифрового неравенства», решение которого является необходимым условием вхождения республики в число 30 развитых государств мира, так как уровень развития информационных и коммуникационных технологий (ИКТ) в стране является одним из существенных индикаторов страны [1]. Необходимо максимально использовать КСС «KazSat» и в плане кибербезопасности информационных технологии путем разработки инновационных наукоемких программ.

Жертвами кибератак становятся предприятия и организации всех масштабов, а экономический ущерб от подобных злонамеренных действий к 2022 г. может достичь 8 трлн. долларов США [2]. Среди известных примеров – недавние кибератаки, которые привели к стагнации работы банковской сферы, закрытию предприятий малого бизнеса и сбоям в предоставлении общественных услуг. Так, в мае 2017 г. пользователи 150 стран мира, в том числе Казахстана, подверглись атаке вируса WannaCry [3]. За возобновление работы каждого компьютера хакеры требовали выкуп в размере $600.

В период участившихся кибератак весьма действенны меры коллективной безопасности. Так, недавно 34 компании в сфере технологий и обеспечения безопасности подписали технологическое соглашение по кибербезопасности (Cybersecurity Tech Accord); это договор между крупнейшей в истории группой компаний, обязующихся защищать клиентов по всему миру от злона-

DOI: 10.24411/2304-9081-2019-11004

меренных действий киберпреступников. Среди компаний-подписантов есть: ABB, Oracle, Nokia, Arm, Cisco, Facebook, HP, HPE и Microsoft. Совместно эти предприятия представляют создателей и пользователей технологий, обеспечивающих работу мировой коммуникационой и информационной инфраструктуры. При этом предусматривается повышенная защита вне зависимости от мотивов и целей онлайн-атак, то есть принятие мер по защите своих продуктов и сервисов от взлома или злонамеренного использования технологической разработки и дистрибуции. Эти коллективные действия будут развивать существующие связи и совместно создавать новые партнёрства с другими представителями отрасли, гражданского общества и исследовательских кругов с целью наращивания масштабов технического сотрудничества, выявления факторов уязвимости, совместного анализа рисков и сведения к минимуму потенциальной возможности появления вредоносных кодов в киберпространстве.

Методы обеспечение надежности функционирования информационных систем (ИС) основаны на использовании аналитико-математических моделей надежности программных средств, которые позволяют сделать оценки зависимости надежности программного средства от определенных параметров. [4, 5]. Эти модели основаны на показателях того или иного поведения программы в момент проведения тестирования. Существуют две аналитические модели: динамические и статистические [6].

Мы произвели оценку и анализ рисков качественными и количественными методами. Качественная оценка риска определялась в соответствии с выбранной шкалой, что позволяет определить необходимые средства и меры защиты. Однако качественный метод не дает конкретной числовой оценки эффективности комплекса контрмер [7]. Используя метод Н.Г. Милославской, М.Ю. Сенаторова, определили зарубежные сайты с использованием инструментальных средств управления рисками информационной безопасности [8]. Метод оценивания критичных угроз, активов и уязвимостей (OCTAVE) имеет ряд модификаций для предприятий различных размеров и видов деятельности [9, 10]. Обнаружение и измерение рисков в информационных системах через диагностические экспертные системы гибкого управления было проведено в работах J. Janulevičius и др. [11]

Безусловно, что управление рисками является весьма трудоёмким процессом, требующим привлечения профессиональных экспертов, но полученные преимущества успешно компенсируют все затраты и потерянное время

DOI: 10.24411/2304-9081-2019-11004

[7]. Особый интерес представляют методы, представленные в исследованиях [12-14], где рассмотрен подход, основанный на оценке рисков и их нейтрализации для повышения надежности информационных систем. Данный подход дает возможность произвести оценку риска на этапе разработки программного обеспечения с уточнением наиболее эффективных стратегий по смягчению рисков, на основе уже существующих данных [15-16].

Обсуждение

Каким образом обстоят дела по кибербезопасности в других странах? Одним из самых продвинутых государств в данной сфере является Россия, здесь 60% компаний имеют свою стратегию защиты и реально используют её на практике. В этом плане она обошла Германию (45%), Францию (51%), Италию (55%) и сравнялась с США (60%). Об этом сообщают «Известия» со ссылкой на отчет консалтинговой компании PricewaterhouseCoopers (PwC) [17]. По данным отчета, наиболее защищенными от кибератак странами являются Малайзия (74%), Япония (72%) и Индонезия (70%). Особенность российских компаний состоит в том, что не все из них используют на практике международные стандарты кибербезопасности, и зачастую отдельные аспекты защиты от киберугроз упускаются. В то же время за границей данные стандарты часто являются обязательными. Согласно отчету, наиболее серьезными киберугрозами в российских компаниях считают нарушение конфиденциальности данных (48%), нарушение нормального хода деятельности компании (47%), снижение качества продукции (27%) и создание угрозы для жизни (21%).

Как отмечается в этом же отчете, большинство сотрудников опрошенных российских компаний назвали фишинговые атаки основными причинами киберинцидентов. На втором месте оказалось использование мобильных устройств – на данную проблему указали более четверти респондентов. Эксперты отмечают, что Россия и США являются мировыми лидерами в сфере кибербезопасности, соответственно могут экспортировать продукты и услуги по защите от киберугроз за рубеж.

Сотрудничество Казахстана со специалистами из Российской Федерации очень своевременно и направлено на консолидацию взаимных усилий, технических и человеческих ресурсов в области защиты от кибератак. В 2017 г. в Алматы состоялось подписание меморандума о сотрудничестве и взаимодействии между компанией Positive Technologies, специализирующейся на

DOI: 10.24411/2304-9081-2019-11004

производстве программного обеспечения в области информационной безопасности, и "Государственной технической службой" Комитета национальной безопасности РК. Сотрудничество направлено на консолидацию взаимных усилий, технических и человеческих ресурсов в области обнаружения, предупреждения и ликвидации последствий кибератак. Страны намерены оперативно обмениваться информацией об угрозах информационной безопасности, распространении вредоносного ПО, новых уязвимостях и средствах их эксплуатации, данными об атаках и атакующих, индикаторами компрометации, а также совместно реагировать на инциденты.

Наиболее популярной технологией информационной безопасности являются автоматизированные средства контроля защищенности информационных систем, управления событиями информационной безопасности и выявления инцидентов. Ожидается, что эти направления обеспечат 70-75% общего объема продаж российской компании на территории РК в ближайший год. Далее будут решения класса application security — средства для анализа исходного кода и защиты вебприложений. Прогнозируемая доля их продаж составляет около 20%. В дальнейшем совместное сотрудничество продолжится в реализации средств многоуровневой защиты от вредоносного ПО, технологии киберзащищенности АСУ ТП компании из энергетической отрасли Казахстана с использованием экспертных сервисных услуг компании Positive Technologies.

Анализ состояния информационной безопасности в Казахстане показывает рост угроз информационной безопасности, в связи с чем экстренно принят ряд кардинальных мер по киберзащите. Так, 9.01.2017 года вступило в силу постановление правительства «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». При этом для определения критически важных объектов информационно-коммуникационной инфраструктуры в стране действуют «Правила и критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры» [18]. Для предотвращения киберугроз реализованы следующие меры:

- создан Комитет по информационной безопасности, координирующий вопросы в сфере обеспечения информационной безопасности;
- созданы Службы реагирования на компьютерные инциденты;

DOI: 10.24411/2304-9081-2019-11004

- развивается нормативно-правовое обеспечение, в частности разработан и утвержден новый Закон РК «Об информатизации», разработаны единые требования в области информационно-коммуникационных технологий и обеспечений информационной безопасности;

- определены стратегические приоритеты развития Казахстана в области информационной безопасности – создание национальной системы «Киберщит»;

- проводится аттестация и испытания на соответствие требованиям информационной безопасности;

- организовано подключение к Интернету через единый шлюз доступа к Интернету, который позволяет значительно сократить количество угроз информационной безопасности и др.

Указанные единые требования это своего рода кодификация из ранее разрозненных норм и гармонизированных в Казахстане технических стандартов в области информационных технологий, защиты информации. Постановление в директивной форме описывает процедуры и правила по использованию информационных технологий при обработке защищаемых законом видов информации, не содержащих государственных секретов [19]. Все указанные меры позволят обеспечить максимально безопасное использование информационно-коммуникационных технологий в республике.

Анализ информационной безопасности в республике Казахстан требует комплексного подхода. При этом необходима последовательность их реализации на основе разработки государственной дорожной карты по кибербезопасности, где приоритетное место должно быть уделено подготовке казахстанских кадров (бакалавров, магистров, докторов PhD), ввиду дефицита квалифицированных специалистов в данном направлении. Должно приветствоваться открытие дополнительных специальностей в вузах, обучающих по программе повышения квалификации в направлении подготовки специалистов, сертифицированных по международным стандартам в области безопасности [20].

Постоянный контроль своевременного устранения уязвимостей, исключения и предотвращения угроз и инцидентов информационной безопасности должно предусматривать:

- развитие отечественной индустрии информационной безопасности, стимулирование отечественных производителей ПО и технических средств;

DOI: 10.24411/2304-9081-2019-11004

- организацию научно-исследовательской и опытно-конструкторской работы в сфере кибербезопасности, развитие отечественных лабораторий по сертификации на отсутствие технических каналов утечки информации;
- разработку национальных стандартов в сфере информационной безопасности, включая гармонизацию с международными стандартами и техническими регламентами;
- развитие международного сотрудничества с внедрением опыта других стран с основами аккредитации и сертификации национальных агентств, либо специалистов;
- разработку стандартов по оценке уровня кибербезопасности в сравнительном аспекте, на основе национальных и отраслевых программ, а также по исследованию и развитию лучших практик по кибербезопасности.

Неисполнение любой составляющей в обеспечении информационной безопасности может привести к повышению рисков реализации негативных последствий. Анализ количества растущих кибератак и инцидентов (более 20 тысяч в год) показывает, что наибольшее количество инцидентов связано с ботнетами – одними из наиболее значительных и постоянно растущих угроз для Интернета, которые могут привести к разрушительным последствиям. Зараженные компьютерные армии могут контролировать компьютеры, даже если их владельцы не знают и не используют их. Ботнеты могут использоваться для спама, фишинга или в качестве шпионского ПО, но наиболее часто они выполняются для реализации атак с распределенным отказом в обслуживании (DDoS). Этот вид кибератак делает недоступным для пользователей интернет-сервис, создавая огромное количество трафика, потребляющего все ресурсы жертвы [21].

Анализ различных технологий процесса обеспечения безопасности автоматических систем (АС), проведенный нами за последние годы, показал, что надежность оценки рисков от кибератак необходимо производить по следующим параметрам и последовательности (табл.). Причем меры обеспечения безопасности АС должны подвергаться оценке в течение всего жизненного цикла системы.

Опыт многих стран использующих стандарты серии ИСО/МЭК 15408 по данной схеме, обеспечивает процесс безопасности АС на основе снижения уровня рисков, методом уменьшения неприемлемых рисков до приемлемого уровня на основе периодической переоценки рисков безопасности АС и спо-

DOI: 10.24411/2304-9081-2019-11004

собности противостоять этим рискам. Наши данные в этом плане целиком и полностью согласуются с выводами [22].

Таблица. Процесс обеспечения безопасности АС на основе уменьшения рисков с применением основ существующих стандартов серии ИСО/МЭК 15408

Оценивание рисков	Идентификация рисков → Анализ рисков → Оценка рисков
↓	↓
Выбор мер безопасности	Выбор мер безопасности в задании по безопасности для системы (ЗБС)
↓	↓
Применение мер безопасности	Применение мер безопасности по отношению к системе как объекту оценки (СОО)
↓	↓
Оценивание рисков	Идентификация рисков → Анализ рисков → Оценка рисков
	↓
Аттестация	Принятие остаточных рисков

Согласно исследованию экспертов, в Казахстане 73% используемого программного обеспечения (ПО) является нелицензионным. Для сравнения, в России этот показатель достиг 64%. Меньше всего нелегального ПО установлено в Чешской Республике – 33%. Это приводит к тому, что ценные данные всегда находятся в зоне риска. Ныне представители крупного и среднего бизнеса в РК уже начали осознавать важность информационной безопасности и приобретения лицензированного ПО. Однако еще значительная часть малого и среднего бизнеса находятся в зоне риска [17].

Актуальность проведения всеобуча «Киберщит» на уровне семинаров, тренингов и круглых столов, где будут рекомендованы использования лицензированного ПО (уровень опасности пиратских версии), не вызывает сомнений. Эти мероприятия проводятся не только для того, чтобы избавиться от «пиратской» культуры, но и для того, чтобы объяснить пользователям риски кибербезопасности, защитить личные данные, финансы и предотвратить возможные убытки. Причем за использование нелегального ПО в Казахстане предусмотрена уголовная ответственность (нарушение авторских и (или) смежных прав), статья 198 УК РК предусматривает штраф до 100 МРП. В более крупных масштабах предусмотрены штраф до 5000 МРП, либо лишение свободы до пяти лет.

DOI: 10.24411/2304-9081-2019-11004

Заключение

Кибербезопасность – сложная транснациональная проблема, требующая международного сотрудничества для обеспечения сети Интернет. Для эффективного противодействия этим угрозам необходима многоуровневая система кибербезопасности, которая защитит наших граждан и государственные институты.

Государство и руководители больших компаний Казахстана должны максимально использовать КСС «KazSat» в плане кибербезопасности информационных технологий путем разработки инновационных наукоемких программ.

Анализ методов и технологий обеспечения безопасности функционирования информационных систем показывает, что в настоящее время известны десятки зарубежных программных продуктов по анализу рисков. Учитывая значимость разработки отечественных программных продуктов, направленных на обеспечение надежности информационных систем, необходимо принять к широкому внедрению разработки методов профессора С.Н. Боранбаева и др., предложенных в работах [11-13], для оценки рисков программных продуктов. Требуется укреплять сотрудничество Казахстана со специалистами из Российской Федерации по консолидации взаимных усилий, технических и человеческих ресурсов в области защиты от кибератак, обмениваться информацией об угрозах информационной безопасности, распространении вредоносного ПО, а также совместно реагировать на инциденты.

Необходима последовательная реализация информационной безопасности на основе государственной дорожной карты по кибербезопасности, где приоритетное место должно быть уделено подготовке кадров (бакалавров, магистров, докторов PhD), ввиду дефицита квалифицированных специалистов в области кибербезопасности. Необходимы институты повышения квалификации в направлении подготовки специалистов, сертифицированных по международным стандартам в области безопасности.

Анализ обеспечения безопасности АС использующих стандарты серии ИСО/МЭК15408 показал надежность автоматических систем на основе снижения уровня рисков, методом уменьшения неприемлемых рисков до приемлемого уровня на основе периодической переоценки рисков и способности противостоять этим рискам.

DOI: 10.24411/2304-9081-2019-11004

ЛИТЕРАТУРА

1. https://www.inform.kz/ru/obespechenie-kiberbezopasnosti-v-kazahstane-vozlozhili-na-sputnikovuyu-sistemu-kazsat_a2993823
2. Moar J. The Future of Cybercrime & Security: Enterprise Threats & Mitigation Sales & Marketing Manager, (2017)
3. https://www.zakon.kz/Sputnik/kak-kazahstan-perezhil-ataku-virusa-wannacry.html
4. Мальков М.В. О надежности информационных систем. Труды Кольского научного центра РАН. 2012. Т.4, №11. Вып. 3: 49-58.
5. Расулова С.С Надежность информационных систем: Конспект лекций. Ташкент: ТашГТУ, 2007. 117с.
6. Швалев И.С., Чусавитина Г.Н., Давлеткиреева Л.З. Сравнительная характеристика автоматизированных инструментальных средств управления информационными рисками. Совр. науч. исследования и инновации. 2012. Т.11 №19. (URL: http://web.snauka.ru/issues/2012/11/18524 (дата обр.: 04.02.2018).
7. Милославская Н.Г., Сенаторов М.Ю. Управление рисками информационной безопасности. М.: Горячая линия-Телеком, 2014. 130с.
8. Агишев Т.Х., Хасанов Ш.А. Инструментальные средства управления рисками информационной безопасности. Матер. межд. научно-практ. конф. «Информационные технологии. Проблемы и решения». Уфа, 2017: 291-295.
9. Староверова Н.А., Фадхкал З. Анализ существующих методов оценки рисков корпоративных информационных систем. Вестник Казанского технол. унив-та. 2013. Т. 16. №9: 282-287.
10. Janulevičius J., Šiaudinytė L., Čenys A., Goranin N. Detection and measurement of information system risks through adaptive management diagnostic expert systems. 12th IMEKO TC10 Workshop on Technical Diagnostics, Italy, Florence, 2013: pp. 45-49.
11. Боранбаев А.С., Боранбаев С.Н., Ерсаханов К.Б., Нурушева А.М. Методы обеспечения надежности информационных систем. Вестн. ЕНУ. 2017. Т.2. №117: 61-70.
12. Боранбаев А.С., Боранбаев С.Н., Ерсаханов К.Б., Нурушева А.М. Выявление потенциальных отказов программного обеспечения и их нейтрализация. Сб. докл. IV Межд. науч-практ. конф., Астана, 2017: 338-340.
13. Boranbayev A., Boranbayev S., Yersakhanov K., Nurusheva A., Taberkhan R. Methods of Ensuring the Reliability and Fault Tolerance of Information Systems. 15th International Conference of Information Technology, Information Technology. New Generations, 2018: 729-730.
14. Grantham L.K., Stone R., Tumer I. Prescribing and implementing the risk in early design (RED) method. In Proceedings of DETC'06, Philadelphia, USA, 2006: 431-439.
15. Krus D.A. "The risk mitigation strategy taxonomy and generated risk event effect neutralization method". PhD thesis. Missouri, 2012. 176p.
16. Boranbayev S.N., Popov P., Altayev S.A. The Usage Of Design Diversity For Software Fault Tolerance And Reliability. Матер. респ. научно-практ. конф. «Проблемы применения современных матем. методов и комп. технологий в инженерных науках и строительстве», Астана, 2013: 237-243.
17. Российские компании сравнялись с американскими по уровню кибербезопасности. (URL: https://www.securitylab.ru/news/489586.php)
18. Постановление Правительства Республики Казахстан от 8 сентября 2016 года № 529 «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры».
19. http://www.zakon.kz/4838230-kak-v-kazakhstane-budut-borotsja-s.html.
20. Боранбаев С.Н., Тасмагамбетов О.К. Формы и методы интеграции информационных систем правоохранительных органов Казахстана. Вестник ЕНУ. 2016. №2: 26-32.
21. Ramanauskait S., Goranin N., Čenys A., Juknius J. Modelling influence of Botnet features

on effectiveness of DDoS attacks, SECURITY AND COMMUNICATION NETWORKS, 2014.
22. Родичев Ю.А. Нормативная база и стандарты информационной безопасности. Учебное пособие. СПб.: Питер, 2018. 256с.

Получена 23 марта 2019 г.

(*Контактная информация:* **Нурушев Мурат Жусыпбекович** – доктор биологических наук, академик РАЕН, Заслуженный деятель науки РК, профессор кафедры экологии Евразийского национального университета им. Л.Н. Гумилева; адрес: 010000, Республика Казахстан, г. Нурсултан, ул. Сатпаева, 2; E-mail: nuryshev@mail.ru)

LITERATURA

1. https://www.inform.kz/ru/obespechenie-kiberbezopasnosti-v-kazahstane-vozlozhili-na-sputnikovuyu-sistemu-kazsat_a2993823
2. J. Moar (2017) The Future of Cybercrime & Security: Enterprise Threats & Mitigation Sales & Marketing Manager, for more information: Jon.King@juniperresearch.com
3. https://www.zakon.kz/Sputnik/kak-kazahstan-perezhil-ataku-virusa-wannacry.html
4. Mal'kov M.V. O nadezhnosti informatsionnykh sistem. Trudy Kol'skogo nauchnogo tsentra RAN. 2012. T.4. №11. Vyp. 3: 49-58.
5. Rasulova S.S Nadezhnost' informatsionnykh sistem: Konspekt lektsiy. Tashkent: TashGTU, 2007. - 117s.
6. Shvalev I.S., Chusavitina G.N., Davletkireyeva L.Z. Sravnitel'naya kharakteristika avtomatizirovannykh instrumental'nykh sredstv upravleniya informatsionnymi riskami. Sovr. nauch. issledovaniya i innovatsii. 2012. T.11 №19. (URL: http://web.snauka.ru/issues/2012/11/18524 (data obr.: 04.02.2018).
7. Miloslavskaya N.G., Senatorov M.YU. Upravleniye riskami informatsionnoy bezopasnosti. M.: Goryachaya liniya-Telekom, 2014. 130 c.
8. Agishev T.KH., Khasanov SH.A. Instrumental'nyye sredstva upravleniya riskami informatsionnoy bezopasnosti // Mater. mezhd. nauchno-prakt. konf. «Informatsionnyye tekhnologii. Problemy i resheniya», Ufa, 2017. – S.291–295.
9. Staroverova N.A., Fadkhkal Z. Analiz sushchestvuyushchikh metodov otsenki riskov korporativnykh informatsionnykh sistem. Vestnik Kazanskogo tekhnol. univ-ta. 2013. T. 16 №9: 282-287.
10. Janulevičius J., Šiaudinytė L., Čenys A., Goranin N. Detection and measurement of information system risks through adaptive management diagnostic expert systems. 12th IMEKO TC10 Workshop on Technical Diagnostics. Italy, Florence, 2013: 45-49.
11. Boranbayev A.S., Boranbayev S.N., Yersakhanov K.B., Nurusheva A.M. Metody obespecheniya nadezhnosti informatsionnykh sistem. Vestn. YENU. 2017. T.2. №117: 61-70.
12. Boranbayev A.S., Boranbayev S.N., Yersakhanov K.B., Nurusheva A.M. Vyyavleniye potentsial'nykh otkazov programmnogo obespecheniya i ikh neytralizatsiya. Sb. dokl. ÍVMezhd. nauch-prakt. konf., Astana, 2017: 338-340.
13. Boranbayev A., Boranbayev S., Yersakhanov K., Nurusheva A., Taberkhan R. Methods of Ensuring the Reliability and Fault Tolerance of Information Systems. 15th International Conference of Information Technology, Information Technology. New Generations, 2018: 729-730.
14. Grantham LK., Stone R., and Tumer I. Prescribing and implementing the risk in early design (RED) method. In Proceedings of DETC'06, Philadelphia, USA, 2006: 431-439.
15. Krus D. A., "The risk mitigation strategy taxonomy and generated risk event effect neutralization method". PhD thesis. Missouri, 2012. 176p.
16. Boranbayev S.N., Popov P., Altayev S.A. The Usage Of Design Diversity For Software

Fault Tolerance And Reliability. Mater. resp. nauchno-prakt. konf. «Problemy primeneniya sovremennykh matem. metodov i komp. tekhnologiy v inzhenernykh naukakh i stroitel'stve», Astana, 2013: 237-243.
17. Rossiyskiye kompanii sravnyalis' s amerikanskimi po urovnyu kiberbezopasnosti. (URL: https://www.securitylab.ru/news/489586.php)
18. Postanovleniye Pravitel'stva Respubliki Kazakhstan ot 8 sentyabrya 2016 goda № 529 «Ob utverzhdenii Pravil i kriteriyev otneseniya ob"yektov informatsionno-kommunikatsionnoy infrastruktury k kriticheski vazhnym ob"yektam informatsionno-kommunikatsionnoy infrastruktury»;
19. http://www.zakon.kz/4838230-kak-v-kazakhstane-budut-borotsja-s.html
20. Boranbayev S.N., Tasmagambetov O.K. Formy i mestody integratsii informatsionnykh sistem pravookhranitel'nykh organov Kazakhstana. Vestnik YENU. 2016. №2: 26-32.
21. S. Ramanauskait, N. Goranin, A. Čenys and J.Juknius.Modelling influence of Botnet features on effectiveness of DDoS attacks, SECURITY AND COMMUNICATION NETWORKS (2014), DOI: 10.1002/
22. Rodichev YU.A. Normativnaya baza i standarty informatsionnoy bezopasnosti. Uchebnoye posobiye. SPb.: Piter, 2018. 256s.

Образец ссылки на статью:

Оспанов Б.И., Нурушева А.М., Нурушев М.Ж. О новых совместных методах защиты от кибератак в Казахстане. Бюллетень Оренбургского научного центра УрО РАН. 2019. 1: 14с. [Электр. ресурс] (URL: http://elmag.uran.ru:9673/magazine/Numbers/2019-1/Articles/BIO-2019-1.pdf) **DOI: 10.24411/2304-9081-2019-11004.**