2. Закон Кыргызской Республики «О биометрической регистрации граждан Кыргызской Республики»
3. Закон Кыргызской Республики «О выборах депутатов местных кенешей Кыргызской Республики»
4. Закон Кыргызской Республики «Об актах гражданского состояния»
5. Национальная стратегия по устойчивому развитию Кыргызской Республикина 2013-2017 гг.
6. Постановление Правительства Кыргызской Республики «О Едином государственном реестре населения Кыргызской Республики и автоматизированной информационной системе записей актов гражданского состояния Кыргызской Республики» от 21 октября 2013 года № 573.
7. Инструкции о порядке биометрической регистрации граждан Кыргызской Республики», утвержденная распоряжением Правительства Кыргызской Республики от 11 ноября 2014 года № 494-р.
8. Решения Национального совета по устойчивому развитию Кыргызской Республики за период 2014 – 2015 годы.
9. Положение о взаимодействии Центральной комиссии по выборам и проведению референдума Кыргызской Республики и Государственной регистрационной службы в период проведения выборов.
10. Отчеты Государственной регистрационной службы в вышестоящие государственные органы за период 2014 – 2017 годы.

Рецензент: д.т.н. Самсалиев А.А.

УДК 004.413.4:338.49

Джалбиев Э. А., Шаяхметова Б. А.
т.и.к., доцент, И.Раззаков атындагы КМТУнин Экономикадагы информациялык системалар кафедрасынын башчысы,
И.Раззаков атындагы КМТУнин Экономикадагы информациялык системалар кафедрасынын магистранты

IT ИНФРАСТРУКТУРАСЫНЫН ТОБОКЕЛДИКТЕРИН БААЛОО ЖАНА АНЫКТОО

Макалада ишкандадагы баалуу маалыматтарды баалоо тобокелдери каралган. 2017 – жылы болуп өткөн жагдай каралган. Маалымат коопсуздугун камсыздоо жана коргоо ыкмаларынын комплекси куралган. Изилдөө тактасында программалоо комплекси жүргүзүлгөн.

Негизги сөздөр: *IT-тобокел, тобокелдиктерди баалоо, изилдөө, тобокелдикти маалымат технологиялары: коркунуч коопсуздугу, маалымат системасы, маалыматты коргоо, тобокелдикке баа берүү системасы маалыматтык-аналитикалык колдоо*

Джалбиев Э. А., Шаяхметова Б. А.
к.т.н., доцент, заведуюший кафедры Информационные системы в экономике КГТУ им. И.Раззакова,

магистрант кафедры Информационные системы в экономике КГТУ им. И.Раззакова

ОЦЕНКА И ВЫЯВЛЕНИЯ РИСКОВ IT ИНФРАСТРУКТУРЫ

В статье рассматривается вопрос выявления и количественной оценке рисков информационной безопасности предприятия. Рассмотрена статистика инцидентов произошедших в 2017 году. Предложена модель угроз, дана методика формирования комплекса защитных мер информационной безопасности. Подробно изложена структурная схема оценки информационной безопасности. Приведено описание программного комплекса и исследовательского стенда.

Ключевые слова: *IT-риск, оценка рисков, риск, Иифомационные технологии: угроза безопасности, информационная система, защита информации, оценка риска, система информационно-аналитической поддержки*

E.A. Dzhalbiev, B.A. **Shayahmetova**
Ph.D., Associate Professor, Head of the Department Information Systems in Economics KSTU n.a. I.Razzakova,
Master of the Department Information Systems in Economics KSTU n.a. I.Razzakova

ASSESSMENT AND IDENTIFICATION OF IT INFRASTRUCTURE RISKS

The article examines the issue of identifying and quantifying the risks of information security of an enterprise. The statistics of incidents occurred in 2017 are considered. A threat model is proposed, and a methodology for the formation of a set of protective measures for information security is given. The structure of the information security assessment is described in detail. The description of the software complex and the research stand is given.

Keywords: *IT Risk, Risk Assessment, Risk, Information Technologies: Security Threat, Information System, Information Security, Risk Assessment, Information and Analytical Support System*

Развитие компьютерных технологий и сети Интернет привело к расширению толкования термина «информационный риск», так сейчас под ним понимают не только риск заражения вирусами и троянами, хакерскими атаками направленными на хищение и уничтожения оборудования, но и не получения прибыли хозяйствующим субъектом. То есть неэффективного использования информационных технологий, предназначенного для повышения производительности труда работников, автоматизации производственных процессов и неэффективного использования основных средств предприятия.

В соответствии с выше сказанным, существующие реалии требуют комплексного подхода к данной проблеме. Это не только проблема IT- специалистов, но и проблема других подразделений принимающих участие в организации процесса управления рисками. Только объеденение усилий риск-менеджмента, внутреннего контроля и аудита, можно провести мероприятия по минимизации информационных рисков. Что соответственно позволит обеспечить надежную и эффективную IT-инфраструктуру предприятия, которая будет отвечать миссии и стратегии предприятия. И только комплексное решение будет направлена на получение высокой эффективности деятельности и минимизации затрат информационной структуры предприятия.

Данная статья рассматривает одну из актуальных проблем связанного с применением информационных технологий в повседневной практике и направлена на рассмотрение вопроса информационного риска как основной составляющей в применении информационных технологий в основной деятельности, а так же оценке и выявлению данных рисков. Для этого применим риск-ориентированный подход, как наиболее полно отвечающий требованиям экономической целесообразности, и отвечающий современным методикам информационной безопасности.

Очевидность внимания к данному вопросу исходит из статистики. Так по итогам 2017 года по оценке специалистов компании Positive Technologies — одного из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений, приведенного в обзоре «Актуальные киберугрозы 2017 – тенденции и прогнозы». Анализ статистики атак основывались на данных и диаграммах приведенные в данном издании.

Распределение инцидентов выглядит таким образом: частные лица - 26% всех атак, это обусловлено популярностью криптовалют, и в основном атаки были связанны внедрением скрытого майнинга; государственные организации – 13%; банки и он-лайн сервисы – по 8%; другие сферы – 15%, к ним были отнесены все атаки которые не смогли однозначно идентифицировать на какую отрасль было направлено. Диаграмма 1.

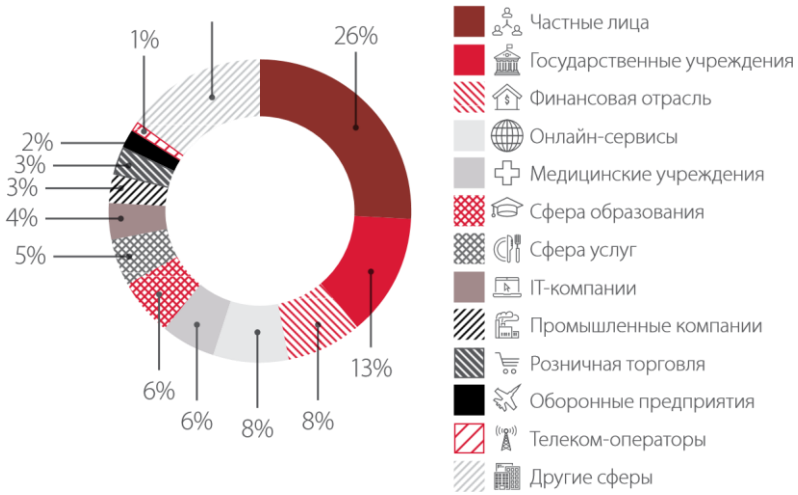

Диаграмма 1. Категории жертв, пострадавших от атак в 2017 г.

Из них по объектам атак, наиболее популярными были инфраструктура и веб-ресурсы – 47% и 26%. Сильно выросло количество атак на банкоматы и POS – терминалы. Структура подробнее показано на диаграмме 2.

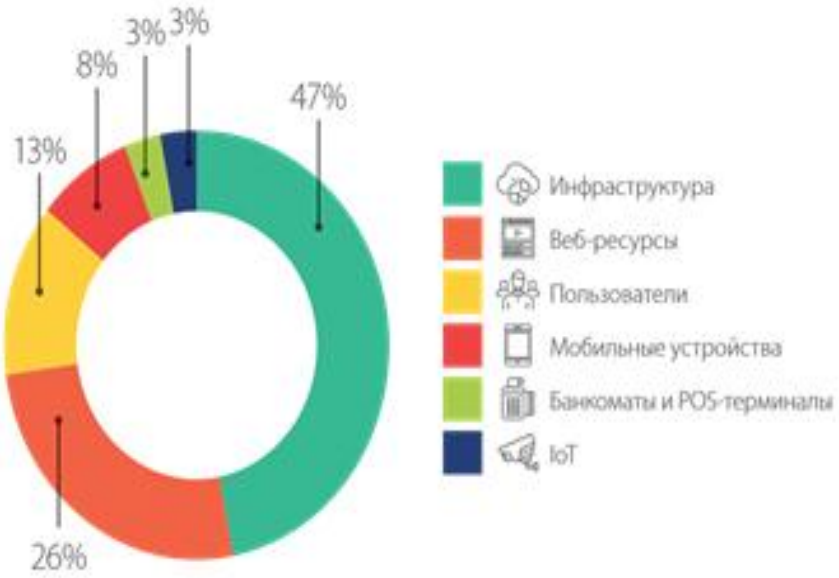

Диаграмма 2. Объекты атак

Основными инструментами при проведении атак злоумышленниками были: вредоносное программное обеспечение (ПО); компрометация учетных данных; уязвимости ПО; социальная инженерия; веб-уязвимости; DDoS атаки и другие методы.

Диаграмма 3. Методы атак

Для построения системы по минимизации информационного риска связанного с методами атак предлагаем, рассмотреть следующие моменты: источники угроз; каким характерным угрозам подвержены, в зависимости от самой инфраструктуры; способы атак и проникновений; уязвимости ПО, операционных систем и характер обрабатываемой информации. На основе этих данных строиться модели угроз присущих применяемой или

разрабатываемой информационной системы. На рис 1 представлена Модель реализации угрозы безопасности информации в ИС.

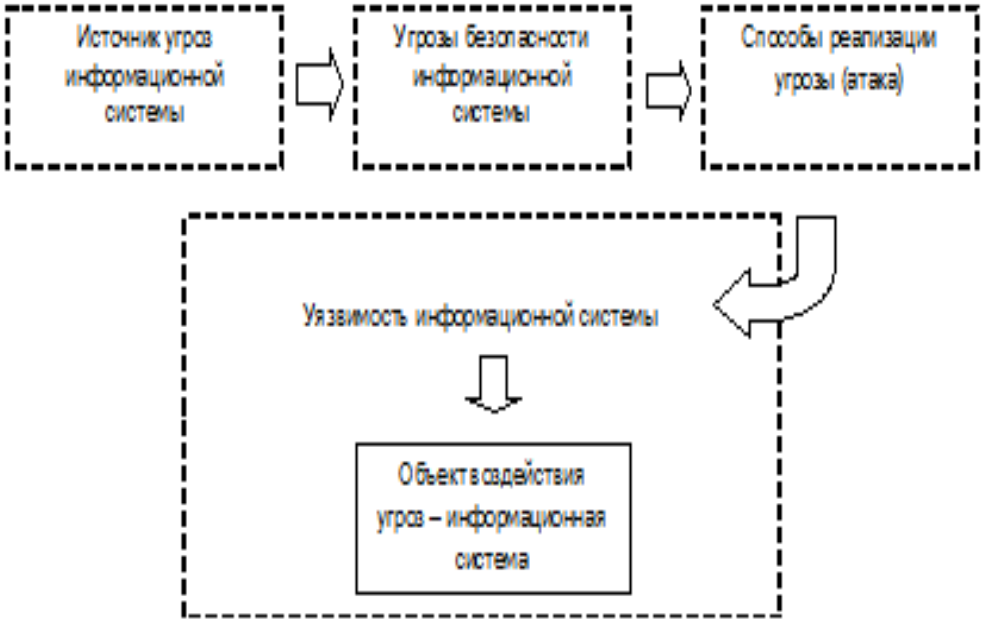

Рис. 1. Модель реализации угрозы безопасности информации в ИС

Но данная модель полностью не отвечает всем требованиям, для полного завершения требуется построить еще Модель нарушителя. И только при совместном рассмотрении этих моделей можно построить отвечающую всем требованиям систему защиты информационной системы. Где Модель нарушителя представляет собой набор предложений об одном или нескольких нарушителях, их квалификации, технических возможностях и материальных ресурсов и т.д.

Сама же оценка риска проводиться на основе имитационного моделирования, методом статистических испытаний (Метод Монте-Карло). Данный метод на наш взгляд более полно отражает количественную оценку риска и он наиболее полно исследован и применен на практике.

На основании разработанных моделей предлагается методика по формированию комплекса мер защиты информационной системы. Данный комплекс мер должен снизить риск информационной системы предприятия, за счет введения защитных мероприятий и мер и так же свести к минимуму ущерб от успешной реализации проникновения. Методика представлена в виде нотации UML на рис. 2.

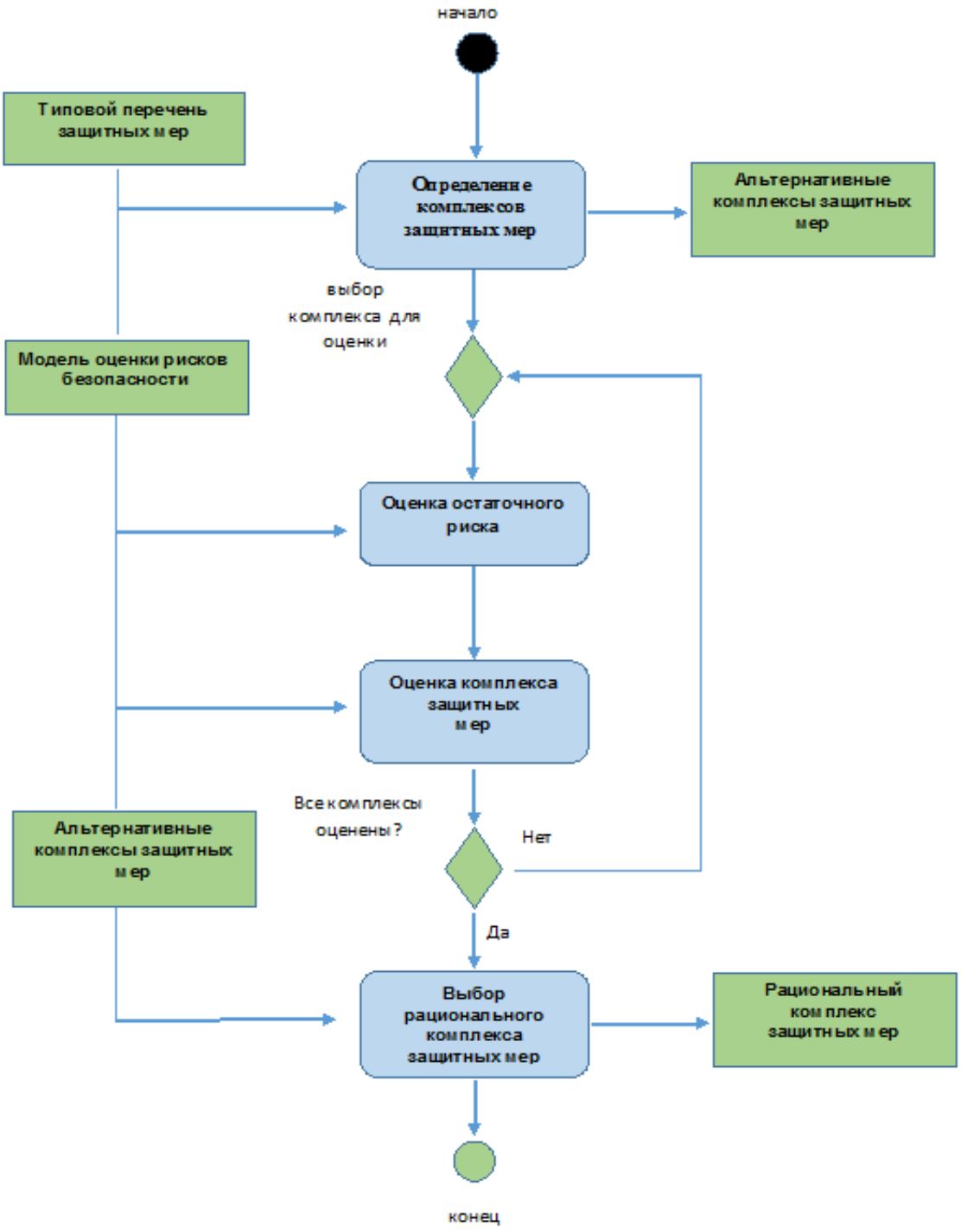

Рис. 2. Методика формирования защитных мер

Структурная схема оценки информационной безопасности приведена на рис. 3. Данная схема представляет собой программную реализацию функциональности модуля оценки риска в системе IT инфраструктуры предприятия или организации. Рассмотрим ее подробнее, она состоит из трех частей: 1 часть модуля, представляет из себя базу данных, в которой формируются данные и записываться все попытки проникновения в информационную систему. На основе данных зафиксированных в базе посредством модуля прогнозирования, в котором программно реализована модель реализации сценариев угроз и построена 3-х слойная нейросеть для расчета весовых коэффициентов, и расчетного модуля в

котором проводятся все расчеты, проводится прогнозирование и оценка риска; 2 часть – предназначена для ввода и вывода информации, в удобной для пользователя виде, а так же реализован интерфейс для связи и вывода информации по требованию пользователей; 3 часть этой схемы представляет собой информационно-справочный модуль.

На основе структурной схемы реализован приложение позволяющая встраивать в любую информационную систему предприятия. В данном приложении, интерфейсы написаны на C#, нейронная сеть реализована с применением программного комплекса Neuro Tools, база данных реализована на SQL сервере.

Для лабораторной оценки и макетирования разработан экспериментальный стенд, реализованный с применением средств MS Excel дополненный Excel-надстройки для нейросетевого моделирования Excel Neural Package. Автоматизация экспериментов реализована с применением VBA Excel. При проведении экспериментов применялся метод статистических испытаний Метод Монте Карло, количество итераций составило 10 000.

В связи с ограниченностью объёма статьи не приведены результаты исследования данного приложения.

Рис 3. Структурная схема оценки информационной безопасности

В связи с повсеместным проникновением информационных технологий в экономику страны, обеспечение безаварийной деятельности информационных структур предприятия стало одной из главных задач. В соответствии с чем информационной безопасности стало уделяться очень много внимания и предприятия тратят значительные денежные ресурсы на обеспечение безопасности своих информационных структур. Одной из главных задач стоящих перед исследователями и разработчиками стало решение задачи обеспечения защиты информационной инфраструктуры с минимальными материальными затратами.

Решение данной задачи невозможно без выявления рисков присущих информационной структуре, а так же ее количественной оценки. Так как количественная

оценка рисков позволяет обосновать материальные затраты на обеспечение защиты IT-структуры предприятия.

Что в свою очередь позволяет внедрить и применять современные и своевременные системы и комплексы защиты. на основе которой соблюдается главный принцип деятельности любой компании или предприятия = непрерывность и безопасность деятельности.

Список использованной литературы:

1. Акимов В. А., Лапин В. Л., Попов В. М., Пучков В. А., Томаков В. И., Фалеев М. И. Надежность технических систем и техногенный риск. М.: ЗАО ФИД «Деловой экспресс», 2002. 368 с.
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. 2008-02-15. М.: ФСТЭК России, 2008. 69 с.
3. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. № 1 (9). 2015. С. 73-79.
4. Варфоломеев А.А. Основы информационной безопасности: учеб. пособие. М.: РУДН, 2008. 412 с.
5. Дулатов И.Н., Ныркov А.П. Современные подходы к оценке рисков информационной безопасности // Материалы III Международной научно-практической конференции «Информационные управляющие системы и технологии». 2014. С. 155-157.
6. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.:Горячая линия –Телеком, 2002. 452 с.
7. Каторин Ю.Ф., Нурдинов Р.А., Зайцева Н.М. Модель количественной оценки рисков безопасности информационной системы // Новый университет. Серия: технические науки. 2016. № 3 (49). С. 42-47.
8. Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). М.: УРСС, 2007. Т. 31. С. 126-207.
9. Мур М. Управление информационными рисками // Финансовый директор. 2003. № 9. С. 64-68.
10. Новикова Г.М. Корпоративные информационные системы: учеб. пособие. М.: РУДН, 2008. 94 с.

Рецензент: д.т.н. , профессор Муслимов А.П.

УДК 656.037.1:336.14.01

Ибраимова С.М., Якупова Н.М.

э.и.к., ЭАИБУнин экономика факультетинин доцентин м.а.
И.Раззаков атындагы КМТУнун “Экономика жана каржы” минбарынын улук окутуучусу

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН БАЖЫ ТӨЛӨМДӨРҮНҮН МАМЛЕКЕТТИК БЮДЖЕТТИН ТҮЗҮМҮНҮН КИРЕШЕСИН ТАЛДОО