ТЕХНИЧЕСКИЕ НАУКИ

УДК 004.387

ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНО-МАТЕМАТИЧЕСКИХ СИСТЕМ

Амирасланова Расмия Исраил кызы
Мингячевирский государственный университет

ASSESSMENT OF INFORMATION SECURITY RISKS USING COMPUTER MATH SYSTEMS

Amiraslanov Rasmiya Israil kizi
Mingechevir State University

РЕЗЮМЕ

Термин «угроза информационной безопасности» (ИБ) относится к ущербу, который могут нанести атаки на системы информационных технологий. Риск ИБ — это широкий спектр потенциальных событий, в том числе утечка данных, меры контроля, финансовые затраты, репутационный ущерб и т. д. охватывает такие вопросы, как ИБ-риски включают в себя аппаратные и программные сбои, человеческие ошибки, спам, вирусы и вредоносные атаки, а также стихийные бедствия, такие как пожары, циклоны или наводнения. Оценка рисков безопасности идентифицирует, оценивает и реализует ключевые элементы управления безопасностью в приложениях. Он также направлен на предотвращение уязвимостей и уязвимостей безопасности программного обеспечения.

SUMMARY

The term "information security threat" (IS) refers to the damage that attacks on information technology systems can cause. IT risk is a wide range of potential events, including data leakage, controls, financial costs, reputational damage, etc. covers issues such as IT risks include hardware and software failures, human errors, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods. The security risk assessment identifies, evaluates, and implements key security controls in applications. The security risk assessment identifies, evaluates, and implements key security controls in applications. It also aims to prevent software vulnerabilities and security vulnerabilities.

Ключевые слова: информационная безопасность, риски информационной безопасности, угрозы, оценка рисков, управление рисками, методология.

Key words: information security, information security risks, threats, risk assessment, risk management, methodology.

Введение.

Надежная работа компьютера в любой сфере деятельности означает, прежде всего, обеспечение безопасности информации, охватывающей эту область. Известно, что существует несколько подходов к оценке уровня информационной безопасности в условиях потенциальных угроз информационным ресурсам. Основными этапами создания систем информационной безопасности являются анализ существующих угроз и оценка рисков информационной безопасности. Процесс анализа угроз безопасности предполагает выявление лиц, событий или процессов, которые могут нарушить конфиденциальность, полноту или доступность информации в информационной системе и иметь недопустимые негативные последствия (ущерб).

Система должна иметь системный подход, который сопоставляет критерии с количественной и качественной оценкой и сравнением рисков для определения их значимости [1]. Основным определяющим фактором при анализе информационных угроз и оценке рисков является выявление источников этих угроз. В большинстве случаев сбои в работе компьютерных систем могут быть вызваны как физическими (аппаратными сбоями), техническими (ошибки пользователя, вредоносное ПО или вмешательство киберпреступников), так и естественными (катастрофы и т. д.) причинами. К наиболее распространенным рискам информационной безопасности в сфере деятельности относятся:

✓Фишинг (Фишинг – обманная схема взлома, при которой пользователи загружают вредоносные сообщения);

✓Вредоносное ПО;

✓Программа-вымогатель (вид вредоносного ПО, предназначенного для вымогательства денег, блокирования доступа к компьютерной системе или предотвращения чтения);

✓Повреждение данных.

✓ Опасные пароли.

Процесс управления рисками информационной безопасности.

Схема управления рискам и представлена на рисунке 1.

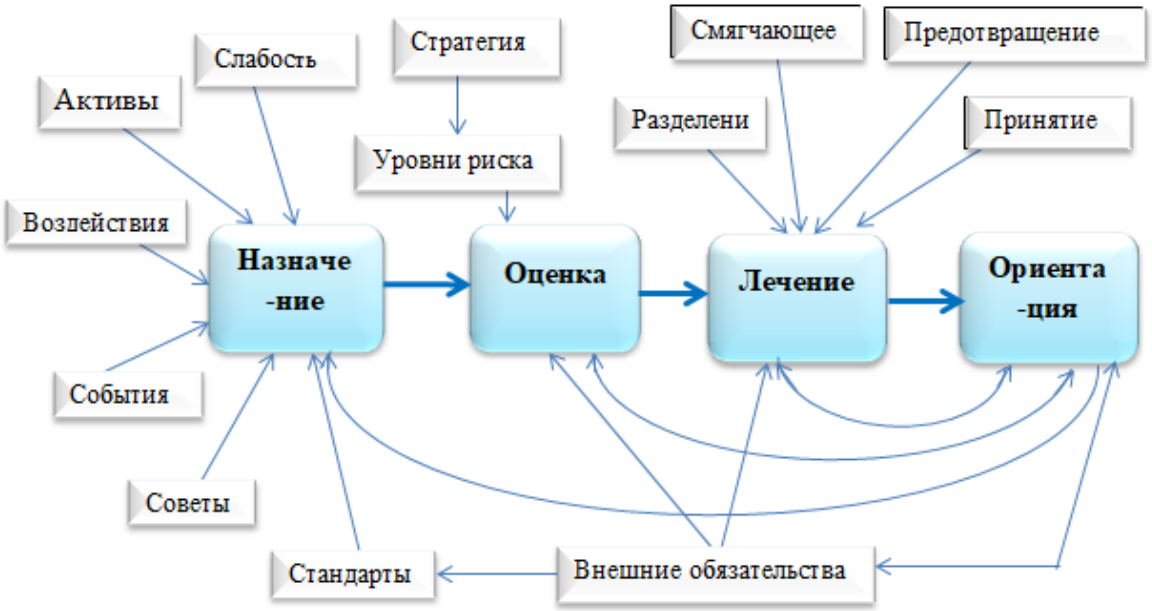

Рисунок 1. Схема управления рисками

Как видно из рисунка 1, управление рисками включает в себя сначала информацию, а затем процесс оценки и управления вовлеченными рисками. Первым шагом в этом процессе является выявление потенциальных информационных рисков. Несколько факторов или источников информации. Следующие этапы включаются в этап «*Назначение*»:

–*Слабые стороны* - слабые места, присущие взаимосвязи между объектами, технологиями, процессами (включая управление информационными рисками), операторами и оборудованием;

–*Угрозы* – это лица (инсайдеры и посторонние) и природные явления, которые могут вызывать инциденты на уязвимостях, вызывающие воздействия;

–*Активы,* информационное наполнение с указанием их актуальности и серверов их хранения, складов;

–*Воздействия* – это неблагоприятные воздействия или последствия происшествий и бедствий, затрагивающие организацию и ее деловые интересы, а часто и третьи стороны, затрагивающие активы;

–*События* могут варьироваться в малом, незначительном или значительном масштабе;

–*Советы, стандарты* и т.д. Применяется к соответствующим предупреждениям и рекомендациям, выпущенным многочисленными организациями, такими как CERT, ФБР, ISO/IEC, журналистами, поставщиками технологий, а также экспертами по информационным рискам и безопасности (наша социальная сеть).

Этап оценки риска включает рассмотрение и оценку всей этой информации для определения важности различных рисков, что, в свою очередь, устанавливает приоритеты для следующего этапа. Толерантность предприятия к риску является здесь серьезной проблемой, и она отражает более широкие культурные факторы и личное отношение профессионалов, участвующих в корпоративных стратегиях и политике, а также в деятельности по управлению рисками.

Обработка рисков означает их предотвращение, смягчение, разделение и принятие. Этот этап включает в себя принятие решения о том, что и как делать (реализация решений по обработке рисков).

Это открытая платформа для важности управления изменениями. Здесь информационные риски постоянно меняются, отчасти в результате обработки рисков, отчасти из-за различных других факторов как внутри, так и вне организации.

В нижней части диаграммы принято, что организация часто должна выполнять внешние обязательства, такие как соблюдение нормативных требований и рыночное давление или ожидания.

Выявление рисков информационной безопасности в компьютерных системах.

Информационный риск — это расчет, основанный на вероятности того, что неавторизованный пользователь негативно повлияет на конфиденциальность, целостность и доступность информации, которую вы собираете, передаете или храните. Известно, что для любой технической системы, в том числе и вычислительной техники, случайные сбои и отказы практически неизбежны [2]. Их образование может быть вызвано как внутренними технологическими причинами, так и внешними факторами (механическими, климатическими, электромагнитными, биологическими, тепловыми и др.). Отказ или сбой могут привести к искажению или даже уничтожению данных, хранящихся и обрабатываемых в системе. Внешние факторы следует учитывать при разработке концепции информационной безопасности для снижения

рисков безопасности с целью минимизации негативного воздействия на окружающую среду. На практике это достигается за счет использования специальных покрытий или применения различных технических мероприятий, таких как герметизация оборудования [3]. Однако технологические меры безопасности, как правило, распространяются только на специализированные компьютерные системы.

Учитывая, что корпоративные компьютерные системы конструктивно менее защищены, они могут подвергаться различным внешним воздействиям, как естественным, так и искусственным. Важно следить за их физическим состоянием во время хранения и обработки данных. Поэтому важно разработать модель оценки рисков информационной безопасности в компьютерных технологиях, используемых на предприятиях.

Определение методики оценки рисков информационной безопасности.

В качестве объекта исследования можно взять согласованные персональные компьютеры или ноутбуки, используемые на предприятиях. Понятно, что на целостность информации и оборудования в компьютерной системе влияют следующие компоненты [5]:

- центральный процессор (ЦП)
- температуры корпуса (материнской платы) и жесткого диска;
- степень влажности корпуса.

Известно, что в компьютерах с дискретным режимом работы температура центрального процессора (ЦП) колеблется в пределах от 450С до 650С. Этот показатель зависит от технологии производства и, в зависимости от производителя, допустимый диапазон нагрева может быть только 30-350С, а при нагрузке 70-750С. В то же время в других случаях температура обычного ЦП может быть 50-550С, а рабочая температура под нагрузкой будет достигать 80-850С, в зависимости от используемой системы кулера (охлаждения).

Температура жесткого диска относительно неравномерна и зависит от ряда условий. Например, зимой температура может быть 40-45 градусов, а летом подниматься до 50 градусов. Основной показатель, который здесь нужно формировать, — это нормальная влажность системного блока. Низкая влажность на уровне 15-20% приводит к накоплению в воздухе статического электричества, что приводит к электризации пыли, загрязнению оборудования и образованию токоведущих дорожек.

Недостаточная влажность (до 30%) приводит к разрушению, высыханию и затягиванию изоляции печатных плат, что в свою очередь приводит к их растрескиванию. Влажность выше 60% вызывает коррозию и окисление контактов, что может привести к короткому замыканию. Рассматриваемые параметры взаимосвязаны.

Температура ЦП может зависеть от состояния термопасты и скорости вращения вентилятора охлаждения ЦП. На температуру винчестера и корпуса влияет установленный на нем вентилятор. Скорость вращения вентиляторов зависит от температуры и регулируется материнской платой. Влажность в корпусе зависит от состояния помещения, что требует установки регулятора в корпусе для ее оценки. Задача комплексного учета совокупности описываемых параметров требует от исследователей наличия специальных знаний и эвристического опыта. Поэтому важно использовать экспертные системы с разумной и соответствующей стратегией при выработке обоснованных мнений о возможных информационных рисках в компьютерной системе [4].

Выводы

Многие концепции безопасности отличаются высоким качеством, и их часто трудно измерить количественно. В ряде случаев экспертная оценка затем оформляется в виде словесных языковых выражений, связанных с числовым (математическим) основанием, что ограничивает возможности технологии, так как экспертная оценка оценки может быть субъективной [6]. Это вызывает необходимость использования лингвистических переменных естественного языка, т. е. аппарата нечеткой логики, оправдывающего себя в обеспечении аналогичной информационной безопасности [7].

В научной работе предлагается методика оценки состояния корпуса компьютера (персонального компьютера или ноутбука) на основе технологии инженерии знаний и механизма нечеткой логики вывода.

Литература

Алесинский Е.И. Применение методов нечёткой логики для решения научной задачи в соответствии с исходными данными // Казань: Молодой ученый. 2021. – № 25 (367). – с. 16-22.

Амирасланова Р.И. Методы и способы обработки и использования данных в компьютерной математике // Москва: Евразийский союз ученых (ЕСУ). – № 10 (67). – 2019. – с. 16-20.

Сахно В. В., Маршаков Д. В., Айдинян А. Р. Применение методов нечеткой логики для решения задачи обеспечения информационной безопасности / Молодой исследователь Дона / № 4 (13), Ростов-на-Дону: Издательский центр ДГТУ. – 2018. – с. 26-34. http://mid-journal.ru

Долженко А.И. Модель анализа риска потребительского качества проектов экономических информационных систем // Вестник Северо-Кавказского государственного технического университета. – 2009. – №1 (18). – с.129-134.

Марков А., Цирлов В. Управление рисками – нормативный вакуум информационной безопасности // Открытые системы. СУБД: Журнал для профессионалов в области информационных технологий. – 2007. – №8. – с. 63-67.

Морозов Д.И. Андреев П.Г., Наумова И.Ю. Защита радиоэлектронных средств от влияния климатических факторов / // Радиоэлектронная техника. Пенза. – 2011. – №1 (4). – с. 255-261.

He, Y., Dai, A., Zhu, J., He, H., & Li, F. Risk assessment of urban network planning in china based on the matter-element model and extension analysis. International Journal of Electrical Power & Energy Systems. – 2011.

УДК 666.263.2: 533.9

ИСПОЛЬЗОВАНИЕ ВТОРИЧНОГО СЫРЬЯ ДЛЯ ПОЛУЧЕНИЯ СТЕКЛОКРИСТАЛЛИЧЕСКИХ МАТЕРИАЛОВ

Волокитин О.Г.,
Скрипникова[1]Н.К,
Кунц[1]О.А.,
[1]Томский государственный архитектурно-строительный университет (ТГАСУ),
Россия, 634003, г.Томск, Соляная пл., 2,
Сабитов[2]Е.Е.
[2]НАО "Евразийский национальный университет имени Л.Н. Гумилева"
Казахстан, 010000, г. Астана, ул. Сатбаева 2, Алматинский район

USE OF SECONDARY RAW MATERIALS FOR OBTAINING GLASS-CRYSTAL MATERIALS

O.G. Volokitin[1],
N.K. Skripnikova[1]
O.A. Kunts,
[1]Tomsk State University of Architecture and Civil Engineering (TSUAB) (Russia, Tomsk)
Russia, 634003, Tomsk, Solyanaya sq., 2,
E.E. Sabitov[2]
[2]NAO "Eurasian National University named after L.N. Gumilyov"Kazakhstan
010000, Astana, st. Satbaeva 2, Almaty district

АННОТАЦИЯ

Исследованы составы для получения стеклокристаллических материалов на основе зол с применением плазмы. Проведен комплекс физико-химических исследований стеклокристаллических материалов различных составов. Выбран оптимальный состав, который характеризовался наилучшими физико-механическими показателями.

ABSTRACT

The compositions for obtaining glass-ceramic materials based on sols using plasma have been studied. A complex of physicochemical studies of glass-ceramic materials of various compositions has been carried out. The optimal composition was chosen, which was characterized by the best physical and mechanical properties.

Ключевые слова: плазма; зола; плавление; кристаллизация; прочность.

Key words: plasma; ash; melting; crystallization; strength.

Стеклокристаллические материалы являются востребованными в строительной отрасли в связи с высокими эксплуатационными характеристиками (прочность и износостойкость, химическая стойкость, способность выдерживать высокие температурные перепады), обеспечивая возможность их широкого применения [1 – 4]. Особенность стеклокристаллических материалов состоит в том, что их полифазная структура включает как кристаллические, так и стекловидную фазы, объемное соотношение которых может меняться в широких пределах.

Производство строительных стеклокристаллических материалов базируется на использовании природного и вторичного сырья. В настоящее время золы ТЭС широко используются для получения строительных материалов различного назначения. Это связано с тем, что химический состав зол в основном представлен оксидом кремния (более 50 %) и алюминия (более 30 %), что позволяет получать кристаллизующийся расплав при его медленном охлаждении [5 – 6]. Таким образом, использование зол ТЭС позволят расширить сырьевую базу для получения стеклокристаллических материалов [7 – 8].

Применение зол ТЭС требует обеспечения высоких температур, так как их температура плавления варьируется в пределах 1640–1680 °С. В практике известно [9 – 10] эффективное использование энергии термической плазмы для плавления тугоплавких природных и техногенных композиций (материалов) с целью получения химически однородных расплавов.

Цель данного исследования: использование энергии термической плазмы для получения стеклокристаллических материалов.

Материалы и методы исследования

В шихтах для получения расплавов содержание золы варьировалось в пределах 60–100%. Дополнительные компоненты известняк и кварцевый песок взяты из условия получения расплавов, обеспечивающих кристаллизацию анортита. Химический состав используемых сырьевых материалов представлен в таблице 1.