УДК 004.056

Информационная безопасность муниципалитетов Забайкальского края и пути ее совершенствования

Кухарский Артем Николаевич
Забайкальский государственный университет
магистр

Аннотация
В статье рассматривается необходимость полного переосмысления взглядов и разработки совершенно новых концептуальных подходов к вопросам информационной безопасности, решения проблем с такими новыми явлениями, как кибертерроризм и киберпреступность для обеспечения информационной и национальной безопасности.
Ключевые слова: информационная безопасность, информационное обеспечение, модернизация, муниципалитеты.

Information security municipalities of Trans-Baikal Territory and the ways of its improvement

Kukharsky Artem Nikolaevich
Transbaikal State University
master's degree

Abstract
The article discusses the need for a complete rethinking of attitudes and the development of a completely new conceptual approaches to information security issues, solve problems with such new phenomena as cyberterrorism and cybercrime for information and national security.
Keywords: information security, information security, modernization, municipalities

Мир социальной повседневности представляет пространство политического риска, в которое погружен социальный субъект, поэтому осмысление сущностных характеристик информационной безопасности важно в целях гармоничного жизнеустройства. На фоне общемирового духовного кризиса порядок общественных отношений, устойчивость общества и его способность к саморазвитию детерминировано балансом активности политических субъектов, обеспечивающих информационную безопасность [5]. Актуальность исследования нормативно-правовых, организационных и управленческих рычагов обеспечения информационной безопасности на современном этапе в условиях интеграции информационных систем обусловлена тем, что проблемы достижения информационной

безопасности традиционно рассматривались, в первую очередь, с технических позиций.

Многие исследователи отмечают, что проблему информационной безопасности ограничивают до проблемы обеспечения защищенности только компьютерной информации. Так в своей работе О.В. Генне предполагает, «что для осуществления эффективных подходов необходимо взаимоувязанное рассмотрение многих факторов информационной безопасности» [3].

Формирование информационной безопасности – комплексная проблема, в которой можно выделить несколько уровней: законодательный (нормативно-правовые акты, законы, стандарты); административный (общего характера действия руководство); программно-технический (технические меры); процедурный (меры безопасности, которые направлены на контроль мер по обеспечению информационной безопасности).

Исходя из этих уровней, существует необходимость становления и развития теоретико-методологических положений и принципов реализации информационной безопасности органами региональных и муниципальных властей. Индивидуальную значимость принимает рассмотрение комплексных вопросов государственного регулирования и координационного управления обеспечением информационной безопасности.

Проблемы государственного регулирования в информационной сфере стали раскрываться в научных публикациях только во второй половине XX в., когда быстрыми темпами развивался международный обмен научно-техническими достижениями. Неоценимый вклад в данную область внесли следующие отечественные ученые: А.Б. Антопольский, Г.Т. Артамонов, И.Л. Бачило, А.Б. Венгеров, Я.Г. Дорфман, Г.В. Емельянов, В.А.Копылов, В.Н. Лопатин, Г.Г. Почепцов, М.М. Рассолов и др. Среди зарубежных ученых можно отметить работы Н. Винер, В. Роберт, Дж. Бенигер, Ш. Уилбур, Дж. Рондфелдт, М. Кастельс, П. Фердинант, Б. Новек.

Для выполнения поставленных целей и решения управленческих задач необходимо провести мероприятия по совершенствованию информационной безопасности, которые предполагают, как административный, так и организационный уровни защиты информации.

Сбалансированное территориальное развитие федеративного государства предполагает создание условий, позволяющих каждомурегиону иметь необходимые ресурсы для обеспечения достойных условий жизни граждан, комплексного развития и повышения конкурентоспособности региональной экономики. Развитие региональных рынков услуг можно рассматривать как императив для снижения территориальных социально-экономических различий до уровня, обеспечивающего баланс их доходной базы и расходных обязательств. В силу этого необходимо обеспечить информационную безопасность муниципалитетов субъектов РФ, в том числе Забайкальского края[9].

Первый уровень защиты информации является административным. Для обеспечения функционирования деятельности по защите информации

необходимо разработать политику информационной безопасности. «Политика безопасности — это набор правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию» [4]. При разработке политики безопасности, она не должна противоречить существующему законодательству и чем надежнее система функционирования, тем строже и разнообразнее должна быть политика по защите информации. В зависимости от выбранной политики нужно выбирать индивидуальные рычаги, обеспечения безопасности. Одним из рычагов является концепция государственной информационной политики. Как отмечает Т.Е.Бейдина: «Концепция государственной информационной политики носит не технический или вспомогательный характер, а регулируется федеральным законом «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» Государственная информационная политика (далее – ГИП) отражает специфику культуры, в т.ч. понимание роли и места губернатора и правительства Забайкальского края в политике и экономике…Подчеркивается многоаспектность ГИП. ГИП – это «особая сфера жизнедеятельности людей, связанная с воспроизводством и распространением информации, удовлетворяющая интересы государства и гражданского общества и направленная на обеспечение конструктивного диалога между ними и их представителями» [1].

Второй уровень по обеспечению защиты информации – это организационный уровень. В данном аспекте существуют мероприятия, помогающие улучшить защиту информации:

– проведение работ по обучению и повышению профессиональных знаний специалистов по работе с современными программными продуктами;

– разработка мероприятий по совершенствованию систем информационной безопасности;

– организация инструктажа каждого специалиста для осознания всей важности и конфиденциальности информации, с которой он работает. Не редко разглашению конфиденциальной информации специалистом предшествует недостаточное знание правил защиты информации.

– контроль соблюдения правил и норм работы специалистов с конфиденциальной информацией;

– контроль соблюдения норм хранения всей документации;

– плановое проведение обсуждений, семинаров, собраний по вопросам обеспечения информационной безопасности;

– плановый контроль обслуживания информационных систем и инфраструктуры на работоспособность;

– включение системного администратора в систему.

Важность организационного уровня подчеркнула Т.Е. Бейдина: «Основными путями совершенствования работы исполнительных органов государственной работы власти Забайкальского края являются укрепление законности, развитие открытости и доступности информации об их

деятельности, что позволит в условиях выстраивания вертикали власти создать основы эффективного взаимодействия органов власти края с органами местного самоуправления и населением» [2].

Кроме того, важны и технические пути совершенствования информационной безопасности, что служит развитию системы. Программные и технические средства представляют собой основные элементы в реализации защиты информации, а для повышения данных средств рекомендуется провести следующие мероприятия:

– Введение паролей пользователей. Для контроля доступа к информационным системам рекомендуется ввести список пользователей, входящих в систему с индивидуальным логином. Данные пароли передать специалистам с соответствующим инструктажем их использования. Также рекомендуется создать срок действия пароля, по истечению которого пользователю необходимо поменять пароль. Ограничить число попыток входа в систему с неверным паролем.

– Разграничение доступа к серверам. Данное разграничение будет контролировать системный администратор, который реализует доступ к соответствующей информации на сервере для каждого пользователя индивидуально.

– Регулярное сканирование систем и обновление антивирусных программ, что позволит обнаруживать вредоносные программы, нейтрализовать причины заражений. Реализовать работы по установке и функционированию средств антивирусной защиты. Для обеспечения данной эффективности необходимо настроить систему антивируса на плановое сканирование системы и обновление баз данных.

Установка на персональный компьютер-сервер сетевого экрана Agnitum Outpost FireWall, данная программа блокирует несекционный доступ из сети Интернет [6]. Существуют следующие преимущества использования сетевого экрана Agnitum Outpost FireWall: реализует контроль соединения персонального компьютера с другими, блокируя внутренний и внешний несанкционированный доступ в систему. Также отслеживает функционирование локальных программ и их взаимодействие,обеспечивая тем самым защиту от несанкционированной активности и от изощренных хакерских методов взлома персональных компьютеров и утечки информации.

Существуют несколько эффективных сканеров, способных автоматически изолировать вирусы и шпионские программы.

Анализ защищенности объектов вычислительной сети. Для реализации данной задачи можно воспользоваться программой «Сканер-ВС» [8], предназначенной для контроля защищенности сетей от внутренних и внешних угроз.

«Сканер-ВС» выполняет следующие функции:

a) обеспечение контроля реализации сертифицированных программных средств защиты информации;

b) создание защищенности загрузки системы;

c) анализ параметров подсистемы обеспечения защиты информации;

d) обеспечение обнаружения слабых мест сервисов;

e) выполнение анализа парольной системы;

f) оценка эффективности механизмов очистки памяти и поиск информации на носителях информации;

g) проведение анализа сетевого трафика.

Также информационной защитой персонального компьютера является программа защиты от спама. Защита от спама пользователей и программного обеспечения осуществляется путем выявления вредоносных почтовых сообщений пользователя. Можно использовать программы antispam - «Spamoed» [7], данное программное обеспечение позволяет блокировать спам на компьютере. Данная программа обеспечивает фильтрацию почты. Основной принцип функционирование заключается в том, что «Spamoed» автоматически блокирует ненужную пользователю электронную почту.

Современным эффективным средством предотвращения потерь информации при отключении электроэнергии является источник бесперебойного питания. Подобное устройство может обеспечить питание всей сети или отдельного персонального компьютера в промежутке времени, достаточного для восстановления подачи напряжения или для сохранения информации. Информационная функция подобных устройств проявляется в виде сигнала, получаемый системой о том, что аппарат бесперебойного питания перешёл на работу от собственного аккумулятора и время данной автономной работы ограничено. Далее персональный компьютер переходит к завершению всех выполняющихся команд и отключается. Большинство устройств выполняет одновременно функцию стабилизатора напряжения.

Криптографическая защита информации обеспечивает режим целостности и конфиденциальности информации при ее передачи по каналам данных. Протоколирование и аудит являются основной частью обеспечения защиты информации. Функционирование данных понятий подразумевает анализ, сбор и накопление команд происходящих в информационной системе.

Функционирование протоколирования и аудита решают следующие задачи:

- обеспечение отчетности пользователей;
- обеспечение воссоздания последовательности событий;
- обнаружение нарушений работы по защите информации;
- предоставление сведений для выявления проблем.

При протоколировании события необходимо записывать, следующую информацию:

- дата события;
- уникальный id-номер пользователя;
- тип события;
- результат действия;

- источник запроса;
- имена задействованных объектов;
- описание изменений в базы данных защиты.

Эффективность системы по защите информации и действий администраторов будет низкой при отсутствии средств анализа, хранения и сбора информации о состоянии информационной безопасности, централизованного управления всеми ее составляющими. Дело в том, что каждое средство защиты является составляющей всей системы политики безопасности, которая на уровне подсистем задается набором параметров и требований. Все элементы подсистемы, средства защиты, а также система информационной безопасности в целом должны соответствовать политике информационной безопасности. Аудит работоспособности системы, всех правил и других элементов в системе информационной безопасности требует наличия средств мониторинга и управления. Для планового анализа данных, и принятия управляющих решений необходимы рычаги мониторинга.

Реализация данных мероприятий позволит:

- разграничить доступ в систему;
- повысить уровень защищенности каждого пользователя;
- внедрить и разработать эффективную политику информационной безопасности;
- уменьшить количество спама;
- блокировать вредоносные атаки через сеть;
- повысить уровень защиты рабочих станций.

Системный подход применим для муниципального управления. Для каждого муниципального района должна быть индивидуально создана политика информационной безопасности с учетом сотрудничества как государственных,так и муниципальных властей. Концептуальные положения обеспечения информационной безопасности органов муниципальной власти включают требования единой нормативно-правовой базы, регулирующей использование и работу с информацией. А также разработку направлений по улучшению защиты информации и создание единой системы электронного документооборота во всех территориальных образованиях и в государстве в целом.

Библиографический список

1. Бейдина Т.Е. Государственная информационная политика в Забайкальском крае // Власть. 2014. №07. С. 36
2. Бейдина Т.Е. Оценка политической власти и политической системы в субъекте РФ // Власть. 2013. №5. С.22
3. Генне О.В. Основные положения стеганографии // Защита информации Конфидент. 2001. №3. С.20-25.
4. Крупский А.Ю., Феоктистова Л.А. Информационный менеджмент: Учебное пособие. М.: Дашков и К°, 2008. 80 с.

5. Эрдынеева К.Г. Политические риски: полисубъектный подход // Научное обозрение. Серия 2: Гуманитарные науки. 2012. № 1-2. С. 32-38.
6. Agnitum Outpost FireWall / [Электронный ресурс]. Режим доступа - http://www.agnitum.ru/support/kb/-article.php?id=1000295&lang=ru (Дата обращения 05.12.2016).
7. Spamoed [Электронный ресурс]. Режим доступа - http://www.spamoed.com/ (Дата обращения 05.12.2016).
8. Сканер-ВС [Электронный ресурс]. Режим доступа - http://npoechelon.ru/production/65/4291?yclid=2819-290500710796405 (Дата обращения 05.12.2016).
9. Erdyneeva K.G., Vasilyeva K.K., Krysova E.V., Nikonova T.V., Fatikhova L.E., Klimenko T.I., Zaitseva N.A., Marfina L.V. The mechanism of state regulation of regional services markets as an imperative to reduce territorial socio-economic disparities // International Review of Management and Marketing. 2016. Т.6. №2. С.274