DOI 10.37882/2223–2974.2020.05.02

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РЕГИОНАЛЬНОМ УПРАВЛЕНИИ НА ПРИМЕРЕ ГОРОДА МОСКВЫ

INFORMATION SECURITY IN REGIONAL MANAGEMENT ON THE EXAMPLE OF THE CITY OF MOSCOW

P. Beldyugin

Summary. The article analyzes the information security in regional administration using the example of the city of Moscow. The research methodology is an analysis of the scientific literature on a given problem, as well as practical domestic experience. The main problems that arise today with the leak of information are considered.

Keywords: information security, management, regional management, information..

Бельдюгин Павел Станиславович
Аспирант, университет «Синергия» г. Москва
beldyugin_pavel@mail.ru

Аннотация. В статье проведен анализ информационной безопасности в региональном управлении на примере города Москвы. Методология исследования — анализ научной литературы по заданной проблеме, а также практического отечественного опыта. Рассмотрены основные проблемы, которые возникают в наши дни с утечкой информации.

Ключевые слова: информационная безопасность, управление, региональное управление, информация.

В наши дни под информационной безопасностью следует понимать практический аспект доступа без тех или иных санкций для осуществления операций исследования, записи, применения и уничтожения информации. В рамках данной статьи мы освятим проблематику информационной безопасности на примере такого региона России, как Москва. Рассмотрим все существующие на 2019 год угрозы, которые могут быть связаны с нецелевым использованием информации, какие уязвимости несет в себе процедура снижения уровня защиты от взломов, атак и иного рода негативных моментов.

Существующие в наши дни механизмы защиты информации находятся в постоянном развитии и соотносятся с проблематикой захвата важных баз данных. Государственные механизмы регулирования также существуют, эффективно взаимодействуют с властными органами, но при этом даже в Москве имеют множество недостатков.

Управление данными на региональном уровне — одна из самых сложных задач, которая входит в компетенцию ФСБ России, а также частных оперативных розыскных групп. По данным на январь 2019 года, экономический ущерб от нанесения вреда за утечку важной для правительства Москвы информации, составил 10 миллиардов рублей за чуть менее, чем полтора года.

Не секрет, что самая ценная информация, которая имеется в распоряжении правительственных органов, касается именно дипломатической службы. В Москве находится более 200 официальных ведомств иностранных государств, культурных центров, посольств, консульств и промышленных групп, которые тем или иным образом связаны с дипломатическим корпусом.

Основные проблемы, которые возникают в наши дни с утечкой информации из Москвы в иностранные государства, заключаются в сложностях выявления в официальных учреждениях дипломатии тех лиц, которые связаны с получением и передачей конфиденциальных сведений. Только за 2017–2018 годы было выявлено не менее 300 случаев злоупотребления в региональном управлении Москвы, которые привели к разным негативным последствиям. Приведем основные:

1. Утеря контроля над разработкой механизма конфиденциальной корреспонденции.
2. Уличение в способах фальсификации некоторых видов документов государственной важности.
3. Несоблюдение федерального закона о государственной тайне от 20 мая 2008 года.
4. Систематизирована классификация секретной информации.
5. Дешифровка приказов в основные государственные ведомства РФ в городе Москве.

Таким образом, информационная небезопасность наносит серьезный удар по репутации московских компаний, представительств и иных групп, которые связаны с зарубежными партнерами договорными обязательствами.

Военная деятельность и дипломатия — это самые распространенные мишени контрразведки, для которых информационная безопасность Москвы — одна из основных сфер деятельности. Даже самый незначительный отток информации способен нанести урон репутации административным органам Москвы, что было зафиксировано в последние годы более 50 раз. Речь идет о многомиллионных потерях в сфере финансов и утечки информации для зарубежных промышленных групп.

Разберемся подробней в проблематике информационной безопасности в сфере финансов и в том, какое влияние они оказывают на увеличение конечной стоимости производства товара в разных секторах экономики. Итак, проблема принята к рассмотрению.

Службы информационной безопасности Москвы справляются со своей работой в должной мере, но, тем не менее, имеют место официальные данные и статистика финансовой убыточности по разным секторам производства. Внедрение мер безопасности на промышленных предприятиях в Москве наносит значительный экономический ущерб и закладывается в конечную стоимость произведенного товара или оказанной услуги. Как правило, данная величина не превышает и 10% стоимости товара, однако, себя полностью окупает.

Связано это с тем, что информационная безопасность наносит урон не только конечному потребителю товара в Москве, но и репутации предприятия в целом. Основные моменты, на которые следует обратить особое внимание:

1. Недопущение транспортировки секретной корреспонденции.
2. Использование шифра как разновидность защиты информации.
3. Использование буферных страховых компаний.
4. Пресечение попыток кражи конфиденциальной информации посредством мошеннических действий.
5. Выявление фальсифицированных документов службами внешней и внутренней безопасности московских предприятий.

Все сказанное нами выше относится к категории злоупотребления доверием и создания прецедентов для недопущения пропажи информации, важной для бизнеса Москвы и правительственных групп.

Но ограничиваться лишь механизмами защиты конфиденциальной системы информационной безопасности в сфере производства и торговли было бы недостаточно. В действительности наша проблематика в условиях Москвы гораздо шире в связи с особой значимостью города как столицы одной из наиболее значимых держав в мире. Таким образом, стоит рассмотреть концепцию информационной безопасности в региональном управлении в свете новейшей проблематики в 21 веке. [1]

1. Защищать информацию стоит отныне в области неавторизованного доступа извне.
2. Защищать интеллектуальную собственность Москвы, которая выражается в наличии вундеркиндов и экспертов высшего класса в сфере экономических знаний, правовых основ и финансово-аналитической экспертизы.
3. Защита информации касательно стоимости управления рисками и иными плановыми достижениями в научно-производственной сфере деятельности.
4. Мультидисциплинарная область защиты от взломов и воровства информации в таких секторах как: технические, организационные, юридические вопросы деятельности.
5. Своевременное уничтожение и передача информации неавторизованным лицам.
6. Успешно противодействовать возникающим угрозам для государственной власти и иных структур города Москвы.
7. Недопущение снижения степеней безопасности и неприкосновенности частной жизни. Следование механизмам подотчетности и проверяемости потока прохождения закрытой от источников влияния информационной составляющей.

Эксперты выделяют следующие разновидности безопасности в сфере информации: конфиденциальность, целостность и доступность. Данные ключевые факторы оказывают определяющее влияние на проблематику информации в 21 веке. Знания, которые раньше передавались в устной и в письменной форме, отныне незащищены.

Связано это с тем, что контроль за поступающей в административные органы Москвы информацией проходит несколько стадий обработки. Сначала она выверяется на конфиденциальность. Это значит, что назначение поступления знаний строго конечно, и никому другому передаваться не может за исключением наличия письменного разрешения абонента.

Целостность — это особенность информации быть именно в том виде доставленной по нужному адресату, в каком она отправлялась из конечного пункта обработки. Это относится и к строгой финансовой отчетности, и к целому комплексу бизнес-процессов, с которыми связана проблематика передачи информации.

Доступность — это еще один критерий информационной безопасности в условиях 21 века в Москве. Доступность в данном случае весьма условна, то есть ин-

формация не должна выходить за определенные рамки и оказывать влияние ни иные категории. Кроме того, под категорией доступности нужно понимать способности разработки таких методов отправки информации, которые бы содействовали декодированию. Это также один из ключевых терминов развития и внедрения информационной безопасности в условиях 21 века. [2]

Признаки незащищенности баз данных следующие:

1. Отсутствие идентификации концептуального определения компонентов.
2. Создание неприоритетных целей безопасности.
3. Отсутствие целей контроля доступа к новым, более глубинным знаниям.
4. Низкий сорт качества информации.

По данным ФСБ в Москве на 2018 год, наличие базовых структурных элементов в сфере доступа к официальной статистике создало предпосылки для увеличения затрат на внедрение самых современных систем безопасности. Без них невозможно контролировать шифрованный поток информации, наказывать виновных лиц в краже конфиденциальных данных, передаче их третьей стороне, делиться терминологией и российскими секретными разработками.

В среднем разоблачение попытки сбора, хранения и передачи секретной информации в Москве обходится региональному бюджету не менее чем в 100–120 тысяч рублей.

Также надо учитывать, что деньги на защиту информационной безопасности поступают из налоговых вычетов жителей Москвы, хотя имеется также правительственный фонд и резервная база, которые содействуют созданию защищенных каналов связи.

С точки зрения системного подхода можно выделить некоторые составляющие процедуры безопасности в информационной сфере. Рассмотрим их. Научная и законодательно-нормативная база знаний. Структурный потенциал подразделений, которые обеспечивают потенциал ИБ. Режимные меры и методы технического характера. [3]

Вышеприведенный перечень процедур составляет важную составляющую информационной безопасности в Москве на 2019 год. Рассмотрим также вариант с эффективной системой безопасности на базе СОИБ (система обеспечения информационной безопасности) как ключевым фактором роста и развития политики конфиденциальности.

1. Необходимость усиления требований национальной безопасности на основе механизмов СОИБ, которые бы регулировали требования защиты информации специально для того или иного объекта.
2. Согласование требований московского и общероссийского законодательства.
3. Внедрение новейших типов стандартизации и методологии на базе комплекса СОИБ.
4. Доведение системы менеджмента информационной безопасности до уровня высокоразвитых стран.
5. Исключение случаев программно-технических сбоев во время защиты информации на основе принципов СОИБ.

Выше приведенную информацию мы можем трактовать как основной способ реализации федеральной программы в Москве касательно обеспечения защитных мер при передаче информации. Главное, на что необходимо обратить внимание,— это, в какой степени передача данных отвечает требованиям Конституции РФ и стран, с которыми происходит обмен конфиденциальной информацией. [4]

Все стандарты информационной безопасности выделяются в четыре наиболее значимые разновидности, которые взаимодействуют друг с другом. Назовем все из этих стандартов: национальные (региональные) стандарты защиты баз данных, рекомендации по ведению принципов стандартизации, методический аспект исследования и международная стандартизация.

Жертвами неспособности контролировать текущее положение дел в сфере стандартных параметров безопасности при передаче данных становятся не только московские промышленные группы, но и государственные корпорации, которые имеют свои представительства в Москве и области. На май 2019 года их создано более 370 из почти 90 стран мира, что свидетельствует о высокой доле привлечения западных инвестиций в российский бизнес.

Тем не менее, проблемы имеются. Некоторые службы безопасности не справляются с возложенными на них обязательствами и подконтрольные им предприятия терпят убытки. Они достигают часто сотен тысяч евро ежегодно, что соизмеримо с западноевропейскими компаниями. [5]

Исходя из сказанного выше, показатель информационной безопасности в Москве пока еще не достиг своего апогея, тем не менее, он значительно лучше работает, чем 10–12 лет назад, и с каждым годом данный показатель становится все выше. Уровень активности криминала в бизнесе Москвы пока еще очень велик, поэтому заботиться об информационной безопасности приходится на высшем уровне и вкладывать значительные финансовые средства в региональные проекты.

ЛИТЕРАТУРА

1. Конституция РФ (принята всенародным голосованием 12.12.1993). Доступ из справ.-правовой системы «Консуль-тантПлюс».
2. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2018 г. № Пр-212 // Российская газета. 2018. № 34. 16 февр.
3. Концепция информационной безопасности администрации Москвы: постановление главы администрации Хабаровского края от 7 февраля 2017 г. № 44.
4. Об утверждении Концепции технической защиты информации на территории Свердловской области: постановление правительства Свердловской области от 31.10.2015 № 940-ПП. Доступ из справ.-правовой системы «Гарант».
5. Об информационных ресурсах и информатизации города Москвы: закон города Москвы от 24 октября 2017 г. № 52 // Ведомости Московской городской Думы. 2017. № 1. Ст. 206.

Журнал «Современная наука: актуальные проблемы теории и практики»

Университет «Синергия»