УДК 65.0
DOI 10.33764/2618-981X-2022-6-186-191

Совершенствование политики информационной безопасности в организации

К. А. Николаева[1]*, *А. В. Шабурова*[1]

[1]Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: cristina.nikolaewa2016@yandex.ru

Аннотация. В данной статье рассматривается актуальная на данный момент проблема политики информационной безопасности в организациях, поскольку в случае отсутствия документа, регламентирующего политику, организации может быть нанесен непоправимый ущерб. Отмечаются различные причинны, по которым создаются риски для организации. В статье говориться о различных средствах и методах, помогающих предотвратить утечку персональных данных, потерю репутации. Актуальность статьи определяется сохранностью персональных данных, предотвращением несанкционированного доступа, выявлением и предотвращением всевозможных угроз, а также повышением уровня защиты информации от угроз. Цель работы заключается в усовершенствовании политики информационной безопасности с учетом выявленных угроз. Целью проводимого анализа является выявление недостатков, угроз и уязвимостей, которые могут привести организацию к потере важной информации.

Ключевые слова: политика информационной безопасности, банк данных угроз, модель угроз, источники угроз

Improving the information security policy in the organization

K. A. Nikolaeva[1]*, *A. V. Shaburova*[2]

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: cristina.nikolaewa2016@yandex.ru

Abstract. This article discusses the current problem of information security policy in organizations, since in the absence of a document regulating the policy, irreparable damage may be inflicted on the organization. Various reasons are noted for which risks are created for the organization. The article talks about various tools and methods that help prevent the leakage of personal data, loss of reputation. The relevance of the article is determined by the safety of personal data, the prevention of unauthorized access, the identification and prevention of all kinds of threats, as well as increasing the level of protection of information from threats. The purpose of the work is to improve the information security policy, taking into account the identified threats. The purpose of the analysis is to identify shortcomings, threats and vulnerabilities that can lead an organization to lose important information.

Keywords: information security policy, threat database, threat model, threat sources

Введение

В последние годы все более актуальна проблема информационной безопасности в организациях. Основная задача информационной безопасности - это сохранность персональной информации, обеспечение защиты информационных данных, предотвращение несанкционированного доступа к различным информа-

ционным ресурсам, а также выявление угроз и уязвимостей. Ключевым инструментом обеспечения информационной безопасности в организациях является политика информационной безопасности. Следуя рекомендациям, содержащимся в литературе по передовой практике, организации часто внедряют широкий спектр механизмов обучения и контроля, чтобы мотивировать сотрудников следовать своей политике информационной безопасности. Однако на сегодняшний день несоблюдение требований политики информационной безопасности остается одной из серьезных проблем для управления информационной безопасностью.

Для исследования использовались несколько точек зрения для объяснения этого феномена несоблюдения, часто строя модели на теоретических основаниях таких как теория рационального выбора (профессор Бурку Булгурку, 2010), теория мотивации защиты или теория планируемого поведения (В. Балакришнан, 2018). Из существующих исследований видно, что такие аспекты, как отношение, социальные ценности и нормы, являются важными элементами для достижения соответствия поведения политики информационной безопасности. Эти описательные характеристики сотрудника усваиваются в профессиональной среде главным образом посредством социальных взаимодействий, таких как имитация поведения других сотрудников.

В современном мире для исправной работы всех организаций требуется качественно построенная и хорошо развитая политика информационной безопасности организации, а также ее совершенствование. В данной работе исследование направлено на изучение имеющейся политики информационной безопасности в организации, проведение анализа возможных угроз и ее усовершенствования.

Цель настоящей работы заключается в проведение анализа угроз в Управлении Росреестра по Новосибирской области (Росреестр) и актуализации политики информационной безопасности. Для оценки угроз безопасности информации использовалась методика, разработанная Федеральной службой по техническому и экспортному контролю [1].

Материалы

Политика информационной безопасности – это совокупность принципов и правил компании, регламентирующих систему и порядок защиты информационных данных и ресурсов.

Чаще всего во исполнение требования регулятора положение о политике информационной безопасности появляется в виде документа. Регулятором в данном случае выступает организация, отслеживающая исполнение регламента и правил работы юридических лиц в разных сферах. В случае отсутствия у предприятия документа, регламентирующего политику информационной безопасности, организация – регулятор в праве применить некоторые санкции к нарушителю, а в случае грубых нарушений – приостановить деятельность предприятия.

Нельзя не отметить, что политика информационной безопасности является неотъемлемой частью некоторых местных и международных стандартов. Очень

важно соблюдение определенных правил и требований, предоставлением которых занимаются внешние аудиторы, отслеживающие работу той или иной организации [2].

Отсутствие политики безопасности порождает негативные отклики, а подобные оценки отрицательно воздействуют на такие показатели, как рейтинг, уровень надежности, инвестиционная привлекательность и т.д. [3].

Использование защитных мер, взаимодействующих с пользователем информационной системой организации, постоянно вызывает негативную реакцию пользователя. Организация подвергается рискам, когда сотрудники относятся с пренебрежением к новым инструкциям [4].

После того, как политика информационной безопасности в организации будет утверждена, необходимо:

1) осведомить всех работников с политикой;

2) осведомить всех новых сотрудников с политикой;

3) разработать инструкции, процедуры, положения и прочие документы, дополняющие политику.

За выполнение политики ответственность несут все пользователи информационных систем организации. Ответственность сотрудников за несоблюдение требований, которые влекут за собой разглашение или утечку информации ограниченного доступа, определяется законодательством Российской Федерации, внутренними нормативными документами предприятия, а также должностными инструкциями работников [5].

Политика информационной безопасности разрабатывается на основе:

– требований законодательства Российской Федерации;

– ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;

– ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью»;

– Постановления Правительства Российской Федерации от 19 января 2005 № 30 «О типовом регламенте взаимодействия федеральных органов исполнительной власти»;

– политики информационной безопасности Управления.

Контроль за выполнением требований политики информационной безопасности осуществляет руководитель подразделения информационной безопасности путем проведения регулярных контрольных мероприятий [6].

Совершенствование политики информационной безопасности в Росреестре

Проблема совершенствования политики информационной безопасности актуальна для Росреестра. Данная проблема актуальна тем, что в современном мире происходят большие объемы утечки информации, в том числе персональных данных. Для того чтобы политика информационной безопасности соответствовала сегодняшнему дню и как можно больше снизила риски, необходимо по-

стоянно производить мониторинг угроз. Для выявления возможных и существующих угроз в Росреестре была построена модель угроз.

Формирование перечня потенциально возможных угроз безопасности информации производится путем выборки угроз, применимых к Росреестру, из банка данных угроз безопасности информации [7].

Защищенность персональных данных является важной составляющей защиты личности. При незаконном доступе третьих лиц к информации, которая относится к персональным данным, может возникнуть угроза хищения информации, потеря репутации. Оценку степени и вариантов угроз обработки данных, относящихся к персональным, в информационных системах персональных данных (ИСПДН) смогли подготовить ФСТЭК России, а также согласовать подготовленные рекомендации для защиты.

Главным документом в области защиты правоотношений является «Базовая модель угроз безопасности». Действия, при которых злоумышленник пытается завладеть информацией, нарушить целостность и сохранность данных, могут привести к ущербу и потери репутации организации [8].

Для обозначения угроз безопасности информации Росреестра используются индексы в формате УБИ.ххх, либо выборка по источнику угроз.

При построении модели угроз, были выделены основные угрозы:

1) угрозы утечки акустической (речевой) информации;

2) угрозы анализа сетевого трафика с перехватом передаваемой по сети информации;

3) угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

4) угрозы выявления паролей;

5) угрозы удаленного запуска приложений;

6) угрозы внедрения вредоносных программ.

В качестве основы для моделирования для Росреестра нами была использована типовая модель угроз безопасности персональных данных, которая обрабатывается в распределенных информационных системах персональных данных, подключенных к сетям связи общего пользования и (или) сетям международного информационного обмена [9].

Формирование перечня вероятных угроз безопасности информации производится путем выборки угроз, применимых к информационной системе Росреестра, из Банка данных угроз безопасности информации, с последующим их дополнением угрозами из перечня потенциально возможных угроз в соответствии с типовой моделью угроз, применимой к данному типу ИСПДН согласно нормативно-методическому документу «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденному 15 февраля 2008 г. заместителем директора ФСТЭК России, при этом допускается группировка угроз, в отношении которых совпадают объекты воздействия или другие параметры.

Для предотвращения рассмотренных угроз, необходимо на постоянной основе проводить мониторинг и аудит безопасности. Также необходимо принимать

во внимание, что помимо проводимого анализа предполагаемых вторжений в режим конфиденциальности, существует немаловажная, а возможно даже и главная угроза технических средств.

Заключение

На сегодняшний день не каждая организация может защитить персональные данные от деятельности собственных сотрудников. У руководства большинства организаций, которые не требуют изучение новых инструкций соблюдения политики информационной безопасности, могут привести к увеличению уязвимых мест и вероятность возникновения утечек персональных данных очень велика.

В данной статье был проведен анализ угроз в Росреестре, а также рассмотрены возможные пути решения для актуализации политики информационной безопасности.

Для рассматриваемой организации Росреестра были выделены такие разделы для совершенствования политики информационной безопасности, как:

1) угрозы внедрения вредоносных программ;
2) угрозы выявления паролей.
3) угрозы внедрения ложного объекта как в информационной системе, так и во внешних сетях.

При несоблюдении правил, связанных с нарушением политики информационной безопасности, любая из угроз может нанести непоправимый ущерб для Росреестра. Руководитель Росреестра, заинтересованный в безопасности информации и персональных данных, должен в первую очередь сам нести ответственность за выполнение политики, а для контроля сотрудников за выполнением политики информационной безопасности руководитель обязан проводить постоянные и обязательные контрольные мероприятия [10].

После того, как политика информационной безопасности в организации будет утверждена, необходимо:

1) осведомить всех работников с политикой;

2) осведомить всех новых сотрудников с политикой;

3) разработать инструкции, процедуры, положения и прочие документы, дополняющие политику.

Проведенный анализ показал, что возможные утечки данных в Росреестре могут произойти из-за несоблюдения сотрудниками требований политики безопасности. Для уверенности в защите данных, которые могут нанести непоправимый ущерб для организации, руководитель обязан проводить постоянный и контроль и анализировать актуальность разработанных политики информационной безопасности и модели угроз.

Для решения рассмотренных проблем необходимо разработать методические рекомендации, которые будут определять порядок и методы выявления угроз информационной безопасности.

Как было отмечено ранее, политика информационной безопасности является неотъемлемой частью некоторых местных и международных стандартов. Также важно отметить, что соблюдение определенных правил и требований,

предоставлением которых занимаются внешние аудиторы, отслеживающие работу той или иной организации, является очень важным показателем [11].

При отсутствии политики безопасности, организации наносится ущерб, который может быть непоправимым. Для предприятия важно соблюдать все инструкции, касающиеся политики информационной безопасности. При их несоблюдении могут пострадать такие показатели, как рейтинг, уровень надежности, инвестиционная привлекательность и т.д.

В данной статье была использована типовая модель угроз безопасности персональных данных, которая обрабатывается в распределенных информационных системах персональных данных, подключенных к сетям связи общего пользования и (или) сетям международного информационного обмена, а также была построена модель угроз для организации, выделены основные угрозы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Александрович Г.Я. Автоматизация оценки информационных рисков компании / Г.Я. Александрович, С.И. Нестеров, С.А. Петренко // Защита информации. КОНФИДЕНТ : информ.-метод. Журн. - № 2 (50), 2003. – 81 с.

3. Ашмарина С.И Экономические проблемы информатизации предприятий промышленного комплекса: монография / С.И. Ашмарина. - М.: Машиностроение-1, 2004. - 260 с.

4. Баронов В.В. Информационные технологии и управление предприятием: учеб. курс / В.В. Баронов, Г.М. Калянов, Ю.Н. Попов. - М. : Компания АйТи, 2006. - 328 с.

5. Грибунин В.Г. Комплексная система защиты информации на предприятии: учеб. пособие для студентов высш. учеб. заведений / В. Г. Грибунин, В.В. Чудовский. - М.: Академия, 2009. - 416 с.

6. Мельников В.П. Информационное обеспечение систем управления: учебник / В.П. Мельников. - М. : Академия, 2010. - 336 с.

7. Чипига А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига - М. : Гелиос АРВ, 2010. - 336 с.

8. Ярочкин В.И. Информационная безопасность / В;И; Ярочкин. -ML: Академический Проект, Мир, 2003. - 640с

9. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков - М. : Кн. мир, 2009. -352 с

10. Шевченко А.В. Управление безопасностью информационных процессов / А.В. Шевченко. - М. : РАГС, 2009. - 138 с

11. Шанъгин В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин – М.: Инфра-М, 2011. - 416 с.