МЕНЕДЖМЕНТ

Разработка мер защиты конфиденциальной управленческой информации в организации

Development of Measures to Protect Confidential Information Management Information in the Organization

DOI 10.12737/2587-9111-2024-12-2-56-60 Получено: 3 февраля 2024 г. / Одобрено: 12 марта 2024 г. / Опубликовано: 25 апреля 2024 г.

Фомичёва И.В.
Канд. экон. наук, доцент,
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»,
Россия, 125993, г. Москва, Ленинградский проспект, д. 49,
e-mail: fiw712@mail.ru

Юдина О.В.
Канд. экон. наук, доцент,
ФГБОУ ВО «Тульский государственный педагогический
университет им. Л.Н. Толстого»,
Россия, 300026, г. Тула, проспект Ленина, д. 125,
e-mail: polyakovaov2006@yandex.ru

Поляков Д.В.
Студент, ФГБОУ ВО «Тульский государственный университет»,
Россия, 300012, г. Тула, пр. Ленина, д. 92,
e-mail: polyakovdi2002@yandex.ru

Fomicheva I.V.
Candidate of Economic Sciences, Associate Professor,
Financial University under the Government of the Russian Federation,
49 Leningradskiy Prospect, Moscow, 125993, Russia,
e-mail: fiw712@mail.ru

Yudina O.V.
Candidate of Economic Sciences, Associate Professor,
Tula State Lev Tolstoy Pedagogical University,
125, Lenina St., Tula, 300026, Russia,
e-mail: polyakovaov2006@yandex.ru

Polyakov D.V.
Student, Tula State University,
92, Prospekt Lenina, Tula, 300012, Russia,
e-mail: polyakovdi2002@yandex.ru

Аннотация

В статье раскрыты основные положения и значимость сохранения конфиденциальных данных в государственном и муниципальном управлении, организационные и технические меры. Внимание уделено взаимосвязи количества управленческой информации в организациях и роста факторов угроз ее вскрытия. В качестве предостережения от внешних и внутренних угроз рассмотрен подход создания механизма обеспечения безопасности секретных данных, а также приведен список документов, регулирующих область технической защиты информации. Предложены направления внедрения системы защиты конфиденциальной информации в системе управления организацией.

Ключевые слова: информация, ценность информации, организационная защита, информационная безопасность.

Abstract

The article reveals the main provisions and the importance of protecting confidential data in state and municipal management, organizational and technical measures. Attention is paid to the relationship between the amount of management information in organizations and the growth of threat factors for its disclosure. As a warning against external and internal threats, an approach to creating a mechanism for ensuring the security of classified data will be considered, and a list of documents regulating the field of technical information protection will be provided. The directions of implementation of the system of protection of confidential information in the management system of the organization are proposed.

Keywords: information, information value, organizational protection, information security.

Защищать данные, информационные активы является главной задачей для государственных органов, ведь это играет решающую роль в обеспечении сохранности конфиденциальной информации и общей национальной безопасности. В рамках деятельности органов власти защитные меры для информации нацелены на ее консервацию в секрете, обеспечение ее неуязвимости и гарантирование доступа к данным, которые они содержат и с которыми работают. Дополнительно эти меры сконцентрированы на поддержании приватности, неделимости и доступности сведений, которые эти учреждения обрабатывают и хранят [7]. В данном направлении широко известны работы таких авторов, как Бабаша А.В [1], Гафнера В.В., Драчев В.О. [2], Громова Ю.Ю. [3], Малюка А.А. [6] и др.

Сегодня компании сталкиваются с необходимостью управления и использования возрастающих объемов данных, что облегчается благодаря уменьшению затрат на вычислительные ресурсы, повышению пропускной способности сетевых соединений и усовершенствованию систем хранения данных. Изменения в потребностях на рынке кибербезопасности демонстрируются на представленном рисунке.

Под угрозой или опасностью утечки информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или

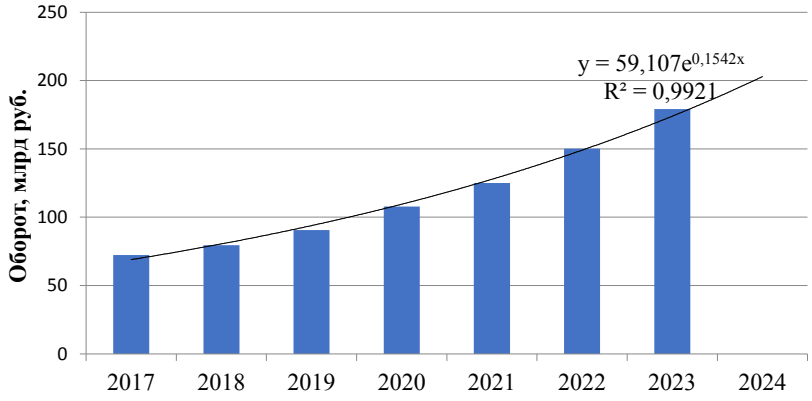

Рис. Динамика и тренд оборота российского рынка информационной безопасности по оценке агентства NAdviser [5]

внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемые и охраняемые ресурсы с массивами данных.

Разглашение конфиденциальных данных способно привести к финансовым убыткам, юридическим последствиям согласно применимым законам, а также порочить репутацию через медийное освещение и внимание со стороны публики. Опасность определяется как сочетание ситуаций и факторов, которые увеличивают вероятность или текущий риск ущерба конфиденциальности, доступа к данным и их целостности.

К частным угрозам защищенности информации относят нарушение ее защиты, модификацию или потерю, неисправности в работе технических устройств и систем управления данными, а также похищение оборудования. Вероятность утечки информации напрямую связана с ее важностью для компании и возможностью такой инцидентности.

Как потенциальные источники риска для защищаемой информации могут выступать не только люди, но и технические средства или программное обеспечение, используемые для обработки, передачи и хранения данных. Помимо этого, определенный риск создают технические устройства и системы, которые косвенно связаны с работой над защищенными данными, а также форс-мажорные ситуации и естественные катастрофы. Чаще всего наибольшую опасность представляет человек, способный нанести ущерб информации как умышленно, так и из-за невнимательности. Среди российских компаний основной проблемой для информационной безопасности становится легкомысленное отношение сотрудников к своим обязанностям, что проявляется в нарушении установленных норм и положений по защите данных на предприятии, что, в свою очередь, может способствовать утечке важной информации различными способами.

К организационным методам обеспечения безопасности информации в структурах государственного управления относятся определение лиц, ответственных за создание и применение стратегий защиты информации, разработка норм и критериев для обработки, сохранения и распространения данных; определение порядка доступа к информационным ресурсам; проведение образовательных и повышающих квалификацию программ для работников; выполнение аудита по информационной безопасности и другие подобные действия.

Чтобы минимизировать риск утечки важной информации, настоятельно советуется проведение опроса новых сотрудников в момент их найма. Этот процесс позволяет оценить умственные способности претендентов, составить мнение о них как о многоаспектных индивидуумах, определить их этико-психологический профиль, обнаружить потенциальную склонность к противоправной деятельности и прочее.

Организация процедуры получения разрешений на работу с секретными данными, являющаяся ключевой частью стратегии управления персоналом, осуществляется на основе определения уровней доступа к персональным документам. Этот процесс включает четкое разделение информации на категории и определение круга лиц, которым эта информация требуется для выполнения своих обязанностей. Выдача разрешений на доступ к секретным данным должна производиться лишь в письменной форме уполномоченным руководителем, что делает его лично ответственным за точность и обоснованность таких действий. Следовательно, менеджмент несет ответственность за корректное предоставление

разрешений на доступ к конфиденциальной информации. В то же время влияние прочих источников потенциальных опасностей зачастую носит случайный характер.

Чтобы избежать распространения секретных данных с применением информационных технологий, требуется техническая защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащих защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Защита цифровых данных часто требует применения методов криптографии. Главная цель криптографической защиты — обеспечение целостности и конфиденциальности данных во время их передачи, предотвращая тем самым возможность их перехвата или изменения. Криптография традиционно направлена на сохранение приватности информации при ее передаче через открытые коммуникационные каналы. Решение этой задачи достигается благодаря криптографическим алгоритмам, установленным между отправителем и получателем информации. Шифрование данных производится исходящей стороной, в то время как получатели применяют процесс дешифрования. Обмен ключами для шифрования осуществляется либо через безопасный канал либо создается общими усилиями пользователей.

В условиях современности обеспечить полную защиту конфиденциальной информации только организационными, программными и техническими средствами нереально. Организационные меры включают стандартизацию рабочих процессов и отношений между сотрудниками на уровне законодательства, минимизируя тем самым риски несанкционированного доступа к данным и снижая угрозы как внутренние, так и внешние. В рамках организационной защиты реализуются меры по обеспечению безопасности, управлению персоналом, документообороту и использованию технических средств безопасности, а также анализу потенциальных рисков.

К важнейшим организационным мерам относятся создание надежного режима и системы охраны, направленных на предотвращение несанкционированного доступа на территорию и в помещения, а также организация эффективной работы с персоналом. В этот процесс входят отбор и распределение сотрудников по их специализациям, проведение тренингов по технике безопасного обращения с секретной информацией, а также информирование о последствиях нарушения предписаний. Более того, особое внимание уделяется управлению документацией и информацией, необходимой для защиты. Это включает организацию процессов создания, применения, регистрации, соблюдения задач, связанных с документацией, их возвращение, архивирование и уничтожение. Происходит управление через применение современных технологий для сбора, анализа, накопления и поддержания безопасности конфиденциальных данных; разработка методов для оценки внутренних и внешних опасностей потери данных и стратегий для их защиты; введение постоянного контроля за деятельностью сотрудников, занятых с конфиденциальными данными, ведение учета, сохранения и утилизации документов и технологических средств.

В каждой организации организационные меры принимают уникальную форму и содержание, которые нацелены на гарантированную защиту информации в соответствии с конкретными операционными требованиями. Современные методы и технологии информационной безопасности, используемые в государственных структурах, включают следующие аспекты: процедуры подтверждения подлинности и предоставления доступа пользователям; криптографическое преобразование информации; создание резервных копий информации и ее восстановление; физическая защита оборудования; регулярное обновление программного обеспечения и установка исправлений; обучение и повышение уровня информационной грамотности сотрудников [7].

Нормативно-правовой фундамент для обеспечения информационной безопасности в учреждениях государственного управления состоит из множества законов и регламентирующих документов, задающих стандарты и указания по охране информации. Важнейшими юридическими источниками в данном аспекте служат следующие законы и нормативные акты: Федеральный закон от 4 мая 2011 г. № 99-ФЗ — «О лицензировании отдельных видов деятельности»; Федеральный закон от 27 июля 2006 г. № 149-ФЗ — «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 27 декабря 2002 г. № 184-ФЗ — «О техническом регулировании»; Закон Российской Федерации от 21 июля 1993 г. № 5485-1 — «О государственной тайне».

Рассмотренные положения материала статьи выступают в качестве предложения для решения следующих задач защиты и путей их реализации.

1. Разработка и реализация программы защиты персональных данных граждан в рамках организационных сервисов:
- создание защищенных баз данных для хранения персональных данных граждан, используемых в организации;
- организация шифрованной передачи данных между различными партнерами микроуровневой среды;
- проведение аудита системы информационной безопасности на предмет соответствия требованиям законодательства о защите информации.

2. Оптимизация управления доступом к информационным ресурсам государственных органов:
- разработка и внедрение системы управления доступом (Identity and Access Management) для контроля за разграничением прав сотрудников на доступ к конфиденциальной информации.

3. Обучение сотрудников организации и ее партнеров правилам работы с конфиденциальной информацией:
- разработка и проведение тренингов и семинаров по информационной безопасности для повышения уровня осведомленности персонала;
- введение регулярных инструктажей о положениях воздействия за пренебрежение нормами управления секретными данными.

4. Анализ и совершенствование мер по обеспечению технической защиты информации:
- внедрение средств защиты информации, включая антивирусы, межсетевые экраны, системы предотвращения вторжений, создание защищенных виртуальных частных сетей (VPN);
- регулярные проверки системы на предмет уязвимостей и адекватности имеющихся защитных мер.

5. Разработка и реализация законодательных и нормативных документов, определяющих процесс работы с секретной информацией:
- разработка и обновление внутренних регламентов и политик безопасности, учитывающих актуальные требования законодательства в области защиты информации;
- приведение политик безопасности государственного управления в соответствие с Федеральными законами и стандартами ФСТЭК.

6. Создание и поддержка бесперебойной работы систем электронного взаимодействия руководства организации с партнерами и клиентами:
- разработка инфраструктуры защищенного электронного взаимодействия руководства организации с партнерами и клиентами;
- внедрение сертификатов электронной подписи для обеспечения подлинности и невозможности отказа от авторства электронных документов;
- создание и администрирование безопасных порталов для подачи заявлений и получения услуг в электронной форме.

7. Контроль за соблюдением правил обработки и хранения конфиденциальной информации в организации:
- аудит и сертификация информационных систем с точки зрения соответствия нормам конфиденциальности;
- реализация решений для защиты записей клиентов в соответствии с требованиями правовых норм о защите данных.

8. Управление киберрисками и инцидентами информационной безопасности в организации:
- разработка и проведение комплексных учений по отработке действий персонала и систем при кибератаках;
- разветвленная система мониторинга за инцидентами информационной безопасности и оперативное вмешательство для их разрешения.

9. Защита инфраструктуры критически важных объектов:
- обеспечение безопасности управления сложными системами, такими как энергетика, транспорт, финансы, путем внедрения специализированных защитных технологий и протоколов;
- сотрудничество с частным сектором для обмена опытом и обучения специалистов по информационной безопасности.

10. Обеспечение прозрачности и открытости данных в управлении организацией при одновременном соблюдении конфиденциальности:
- разработка методик и стандартов публикации открытых данных, обезличивание персональных и конфиденциальных сведений перед их размещением в открытом доступе;
- создание и поддержка платформ для открытых данных, которые обеспечивают легкий доступ к информации и продвигают принципы прозрачности управления.

Литература

1. *Бабаш А.В.* Информационная безопасность. М.: КноРус, 2016. — 136 с.
2. *Гафнер В.В.* Информационная безопасность. Ростов н/Д.: Феникс, 2017. — 324 с.
3. *Громов Ю.Ю., Драчев В.О., Иванова О.Г.* Информационная безопасность и защита информации. Ст. Оскол: ТНТ, 2017. — 384 с.
4. *Запечников С.В., Милославская Н.Г., Толстой А.И.* Информационная безопасность открытых систем. В 2-х т. Т. 2 Средства защиты в сетях. М.: ГЛТ, 2018. — 558 с.

5. Информационная безопасность в России и в мире. https://radio-sgom.ru/advice/proveraem-informaciu-na-dostovernost (дата обращения: 02.02.2024).
6. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.: ГЛТ, 2016. — 280 с.
7. Основы защиты информации в государственных органах: важность и методы обеспечения безопасности // Научные Статьи.Ру — портал для студентов и аспирантов. URL https://nauchniestati.ru/spravka/zashhita-informaczii-v-organah-gosudarstvennoj-vlasti/ (дата обращения: 02.02.2024).

References

1. Babash A.V. Informatsionnaya bezopasnost. M.: KnORus, 2016. — 136 c.
2. Gafner V.V. Informatsionnaya bezopasnost. Rn/D: Feniks, 2017. — 324 c.
3. Gromov YU.YU., Drachev V.O., Ivanova O.G. Informatsionnaya bezopasnost i zashchita informatsii. St. Oskol: TNT, 2017. — 384 c.
4. Zapechnikov S.V., Miloslavskaya N.G., Tolstoi A.I. Informatsionnaya bezopasnost otkrytykh sistem. V 2-kh t. T. 2 Sredstva zashchity v setyakh. M.: GLT, 2018. — 558 c.
5. Informatsionnaya bezopasnost v Rossii i v mire. https://radio-sgom.ru/advice/proveraem-informaciu-na-dostovernost (data obrashcheniya: 02.03.2024).
6. Malyuk A.A. Informatsionnaya bezopasnost: kontseptualnye i metodo-logicheskie osnovy zashchity informatsii. M.: GLT, 2016. — 280 c.
7. Osnovy zashchity informatsii v gosudarstvennykh organakh: vazhnost i metody obespecheniya bezopasnosti // Nauchnye Stat'i.Ru — portal dlya studentov i aspirantov. URL: https://nauchniestati.ru/spravka/zashhita-informaczii-v-organah-gosudarstvennoj-vlasti/ (data obrashcheniya: 02.03.2024).