УДК 65.011.56

РЫБИН ИЛЬЯ ОЛЕГОВИЧ,
ГРАФОВ АЛЕКСАНДР АЛЕКСАНДРОВИЧ

СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И СОБЛЮДЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ

АННОТАЦИЯ

Дана подробная характеристика конфиденциальной информации. Описаны программные продукты, которые применяются для защиты информации в современных условиях. Сформулированы требования для сотрудников организаций по обеспечению конфиденциальности данных. Перечислены основные правила обработки ценной информации, а также делается вывод о необходимости не только установки в организациях специализированных программ, но и соблюдения их персоналом инструкций при работе с любой информацией, особенно с той, которая содержит в себе конфиденциальные данные.

Ключевые слова: конфиденциальная информация; экономическая безопасность; информационная безопасность; обеспечение защищенности; коммерческая тайна.

RYBIN I.O.,
GRAFOV A.A.

WAYS OF PROVIDING INFORMATION SECURITY AND CONFIDENTIALITY UNDER CONDITIONS OF DIGITALIZATION

ABSTRACT

A detailed description of confidential information is given. Software products that are used to protect information in modern conditions are described. Requirements for employees of organizations to ensure data confidentiality are formulated. The main rules for processing valuable information are listed, and the conclusion is made that it is necessary not only to install specialized programs in organizations, but also to make personnel follow the instructions while working with any information, especially those that contain confidential data.

Keywords: confidential information; economic security; information security; ensuring security; trade secret.

Защита информации – первостепенная задача любой организации в современных реалиях экономики. Любая, даже незначительная деталь о технологии производства или о грядущих переменах в организационной структуре может привести к серьезным последствиям не только в долгосрочной, но и краткосрочной перспективе. Именно поэтому так необходимо иметь четкое понимание как защитить необходимую информацию, а также конкретно обозначить степень и уровень защиты того или иного вида информации.

Ущерб от утечки информации проявляется в различных сферах деятельности организации. Примером может служить потеря конкурентных преимуществ или упущенная выгода, а также возможны санкции со стороны государства или иных регулирующих органов за несанкционированное раскрытие персональной или конфиденциальной информации. [1] Урон также может быть нанесен имиджу и бренду компании, что может повлиять на взаимодействие, как с контрагентами, так и с конечным потребителем.

Прежде всего необходимо обозначить что такое «информация». Информация – сведения (сообщения, данные) независимо от формы их представления [2]. Таким образом, из определения понятия информация можно сделать вывод, что это не только конкретные символы, которые формируют данные. Все, что мы каким-либо образом можем зафиксировать, запомнить, услышать или увидеть и, в последствии, использовать – будет считаться для нас информацией. Именно поэтому так важно ограничивать круг лиц, которые будут иметь доступ к той или иной информации, поскольку есть вероятность, что полученная ими информация будет неправильно интерпретирована, либо использована во вред, либо по незнанию, либо преднамеренно. Понимание этого факта и привело к появлению термина «конфиденциальная информация»

Тем не менее, в законодательстве Российской Федерации отсутствует четкое определение для термина «конфиденциальная информация». В зависимости от того, к какой сфере относится или может относиться та или иная информация можно выделить различные виды закрытой информации, или тайн. Так выделяют государственную, коммерческую, налоговую, военную, личную, семейную,

телефонных переговоров (почтовых, телеграфных и иных сообщений), служебную, банковскую тайны и другие. [3]

В современном мире уже все больший и больший упор делается на электронный документооборот. Компании по всему миру переходят от бумажных документов к электронным данным. Создают огромные массивы информации о своих организациях и пытаются обеспечить их защиту. Несмотря на обширное разделение защищенной информации по различным сферам деятельности, принцип защиты такой информации практически одинаков.

События от технических (программно-аппаратных) систем обеспечения информационной безопасности являются важным поставщиком сведений о процессах, происходящих в управляющей системе, об угрозах и рисках. Большое развитие получили системы обнаружения и предотвращения вторжений (IDS, IPS) встраиваемые в современные межсетевые экраны (МЭ), применяемые для обнаружения сетевых атак, эксплойтов и руткитов; системы предотвращения утечек по каналам передачи данных (DLP); различные программно-аппаратные средства и комплексы, контролирующие состояние ЛВС, информационные потоки от различных источников событий и действия пользователей (SIEM). Современные тенденции развития средств обеспечения ИБ демонстрируют переход от узкоспециализированных программных продуктов к комплексам, решающим сразу ряд задач по обеспечению ИБ (например, межсетевые экраны с модулями IPS), что значительно повышает эффективность получения данных об ИИБ и состоянии системы защиты информации в общем виде [4].

Таким образом можно выделить основные виды защиты от утечек информации в организации:

1. Мониторинг каналов передачи данных и использование программ по предотвращению утечек данных (Data Loss Protection/DLP):

Для формирования контроля за основными каналами обмена информацией в организации, включая электронную почту, различные файлообменники, Интернет и соцсети, съемные носители и другие средства связи, используются программы по предотвращению утечек данных, или DLP (Data Loss/Leakage Prevention). В первую очередь они предназначены для того, чтобы информация, которая используется внутри организации не попала в свободный доступ. С помощью таких систем отдел информационной или экономической безопасности может следить за тем, чтобы та или иная информация не ушла в чужие руки. Также с их помощью можно выявлять инсайдеров, продающих информацию и тех, кто потенциально работает на конкурентов, предоставляя им все необходимые данные об организации, в которой они заинтересованы.

DLP-система контролирует все потоки информации на устройстве, на котором она установлена, такие как электронная почта, мессенджеры, интернет браузеры, истории запросов, переданные или скачанные файлы, а также введенные на клавиатуре данные. Система актуализирует информацию, выявляет ее важность, а затем расставляет приоритет по сохранению той или иной информации, того или иного файла на компьютере в зависимости от необходимости сохранения конфиденциальности данных. В случае если алгоритм программы заподозрит утечку, то в автоматическом режиме операция, которая вызвала подозрение будет заблокирована, одновременно с этим будет оповещен отдел безопасности для последующего расследования.

Использование этого программного продукта позволит организации не только сохранить данные, но и также определить отправителя. Если, например, сотрудник организации принял решение передать информацию третьим лицам, система сможет опознать такое действие и сохранит эти данные в архив. Эти действия позволят проанализировать информацию, в любой момент взяв ее из архива, обнаружить отправителя или устройство, с которого была совершена отправка, установить, куда и с какой целью эти данные отправлялись.

В итоге система DLP – это комплексный программный продукт, который обеспечивает высокую надежность сохраненных данных, а также позволяет обеспечить мониторинг защиты данных в организации, выявление нарушений и поиска виновных в тех или иных утечках информации. Такого рода системы могут устанавливаться не только для организаций, в которых большое

количество сведений, не подлежащих разглашению, но также они могут использоваться для охраны:

1. частных сведений организации;
2. интеллектуальной собственности;
3. финансовых данных;
4. медицинской информации;
5. персональной информации сотрудников
6. данных банковских карт и других данных

2. SIEM-системы

Другим эффективным способом обеспечения безопасности информации можно считать программы SIEM (security Information and Event Management). Эта программа позволяет агрегировать и привести к общему виду весь массив данных, который находится на различных ресурсах и иных источниках.

В случае если угроза не была своевременно выявлена, но при этом система безопасности сработала и отразила атаку, то SIEM система соберет все данные, сохранит их и будет держать в памяти в течение определенного отрезка времени. Это позволит воспользоваться этими данными в любой момент времени и провести анализ полученных данных.

Кроме того, такая система позволяет более эффективно отслеживать происшествия, поскольку она отсеивает менее значительные и ставит в приоритет более значимые события.

Пользователь задает специальный фильтр, в котором описаны те события, которые система должна считать подозрительными. При накоплении определенного количества подозрительных событий система оценивает риск и оповещает пользователя о потенциальной угрозе.

3. Ограничение доступа пользователей к информационным ресурсам компании (а также автоматизация процесса согласования и выдачи прав для получения доступа к информации):

В этом пункте большую роли играет ограничение круга лиц, которые имеют полный доступ ко всей информации организации. Необходимо ограничить доступ к файлам и документам для того, чтобы снизить риск утечки информации. Кроме того, рекомендуется включать норму о неразглашении конфиденциальной информации и коммерческой тайны в трудовой договор (контракт) как руководителя организации, так и других сотрудников.

Работники должны быть предупреждены об ответственности, которая на них возложена при работе с конфиденциальной информацией, а также с рисками, которые связаны с утечкой такой информации. Работодателю необходимо предусмотреть порядок и сроки ознакомления сотрудников с должностной инструкцией по работе с закрытыми данными и сохранению конфиденциальности информации для того, чтобы минимизировать риски и создать защищенную среду в организации. Следует разработать специальный документ для сотрудников организации, который будет описывать важность сохранения конфиденциальности информации, а также будет содержать в себе санкции, которые будут применяться, в случае утери данных ответственным лицом. После подписания такого документа, лица, которые имеют отношение к конфиденциальной информации в организации, не смогут использовать полученные в ходе своей работы сведения без согласия руководства или без применения к ним соответствующих санкций. Желательно включить пункты о соблюдении конфиденциальности информации во все документы, которые выполняют кадровые функции, а также обеспечить выполнение данных пунктов техническими средствами защиты.

Если рассматривать литературу по данной теме, то можно обратиться к порядку действий сотрудников отделов организаций, который сформулировали Графов А.А и Мордовец В.А., а именно: «На сегодняшний день разработан и внедрён на практике порядок действий сотрудников отделов организаций, принимающих участие в расследовании инцидента нарушения режима ИБ, которого придерживаются авторы данного исследования:

1. Получение информации об ИИБ;
2. Проверка полученной информации;
3. Принятие экстренных мер (например, срочное отключение питания сервера, подвергнутого атаке злоумышленником);
4. Разработка приказа о создании группы по расследованию инцидента, её выезд на объект;
5. Сбор информации ИИБ на месте;
6. Разработка доказательной базы, изъятие жёстких дисков и журналов записей операционных систем, разработка акта;

7. Анализ полученной информации и разработка отчетных форм для сотрудника, принимающего административные решения;
8. Определение степени вины персонала и оценка ущерба, нанесённого хозяйствующему субъекту» [4].

Исходя из практики применения организациями различных систем защиты информации, можно сделать вывод, что только программных продуктов недостаточно для обеспечения безопасности информации. Сотрудники организации должны соблюдать определенные действия при работе с любой информацией, особенно с той, которая содержит в себе конфиденциальные данные. Сделать это можно, если соблюдать несколько основных правил:

1. Обязательная маркировка документов

Документы, как бумажные, так и электронные, которые содержат конфиденциальную информацию, должны подлежать обязательному маркированию путем проставления грифа конфиденциальности в правом верхнем углу титульного листа.

Маркировка документов должна осуществляться человеком, который их подготовил, либо лицом, ответственным за маркировку документов. Маркирование сообщений, которые были отправлены с электронной почты, должна осуществляется пользователем, осуществлявшим отправку данных сообщений.

Также, в документах, которые передаются третьей стороне и содержат в себе конфиденциальные данные, в обязательном порядке, должно находится «соглашение о конфиденциальности» на обороте титульного листа.

2. Закрытость обсуждений конфиденциальной информации

Данное правило необходимо для того, чтобы на собраниях, на которых обсуждается информация, которая содержит какие-либо конфиденциальные данные не присутствовало лиц, которые не имеют доступа к таким данным. Более того, для соблюдения этого пункта, в организации необходимо выделить и оборудовать специальную переговорную комнату либо зал, который был бы защищен от внешних воздействий, наблюдения или прослушивания. В такой комнате в обязательном порядке должны быть закрыты окна, а также осуществляться проверки на предмет прослушивающих устройств перед каждым заседанием.

3. Шифрование информации при хранении и передаче

Факт шифрования особенно важен для организаций, которые имеют дело с электронным документооборотом. Шифрование поможет обеспечить безопасность данных не только при передаче, когда данные наиболее уязвимы для внешних воздействий, но и во время хранений важных данных, так как в случае успешной попытки взлома архива или базы данных организации, злоумышленники не смогут ими мгновенно воспользоваться, так как данные будут зашифрованы. Это даст время провести внутреннее расследование, выявить утечку или источник взлома, отследить его и, по возможности, сохранить утраченные данные от разглашения или минимизировать потери, понимая какая именно информация была утрачена.

4. Использование соглашения о конфиденциальности

Соглашение играет большую роль во взаимодействии двух сторон, во время пользования информации, составляющей конфиденциальные сведения. По сути, это юридическое ограничение, нарушив которое, сторона будет вынуждена ответить по договору и возместить потери, которые случились из-за этого нарушения. Также к этой стороне будут применены санкции, в соответствии с соглашением о конфиденциальности.

5. Ограничение доступа к информации

Данный пункт подразумевает под собой то, что необходимо ограничить круг лиц, которые бы имели доступ к информации, которую можно считать конфиденциальной. В зависимости от степени важности данных, доступ к ним должно иметь меньше человек, так как от этого напрямую зависит риск утечки данных. В случае, если утечка все же произошла, будет проще проводить расследование, так как количество лиц, которые бы имели доступ к информации будет невелико.

6. Информирование

Это один из самых главных пунктов в списке, поскольку без информирования сотрудников организации о правилах работы с конфиденциальной информацией нельзя ожидать их соблюдения. Каждый сотрудник, который работает с так называемой закрытой информацией обязан знать,

как именно происходит защита, обеспечивать ее, а также должен быть привлечен к ответственности, при нарушении четкого свода пунктов по соблюдению безопасности информации в организации.

Таким образом, при выполнении и систематическом мониторинге соблюдения данных правил можно минимизировать риски утечки информации в организации, а также обеспечить безопасную передачу данных и их хранение.

Список литературы

1. Федеральный закон «О персональных данных» N 152-ФЗ от 27.07.2006.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Указ Президента РФ N 188 от 06.03.1997. «Об утверждении перечня сведений конфиденциального характера»

4. *Графов А.А., Мордовец В.А.* Минимизация ущерба хозяйствующему субъекту путём управления инцидентами информационной безопасности // Журнал правовых и экономических исследований. – 2019. – № 2. – С. 143–147. [Электронный ресурс]. – Режим доступа: http://giefjournal.ru/sites/default/files/024.%20A.A.%20Grafov,%20V.A.%20Mordovets.pdf (дата обращения 18.12.2019)

Статья поступила в редакцию 21 декабря 2019 г.
Принята к публикации 16 марта 2020 г.

Ссылка для цитирования: Рыбин И. О., Графов А. А. Способы обеспечения безопасности и соблюдения конфиденциальности информации в организациях // Национальная безопасность и стратегическое планирование. 2020. № 1(29). С. 71-75. DOI: https://doi.org/10.37468/2307-1400-2020-1-71-75