www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2023.4.6

УДК 004.056:658
ББК 32.972.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Владислав Георгиевич Яриков

Кандидат педагогических наук, доцент,
кафедра информационной безопасности
Волгоградский государственный университет
yarikov.vladislav@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Максим Викторович Пашков

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-221_992475@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В силу развития информационных технологий, в век, когда изменилась ценность информации, последняя стала не только источником знаний, но и предметом посягательств. В масштабах государства, на уровне крупной корпорации или предприятия малой формы хозяйствования, информация играет ключевую роль в обеспечении безопасности.

Ключевые слова: защита, система, безопасность, информация, технологии.

В практике ведения хозяйственной деятельности каждое предприятие сталкивается с тем, что накапливает и обладает информацией, которая носит строго персонализированный характер, не предназначенный для открытого доступа. Такая информация носит конфиденциальный, секретный характер, а также может являться предметом коммерческой тайны или же затрагивать личные аспекты жизни.

Зачастую такая информация может стать предметом преступного посягательства, что предполагает, что такая информация должна быть в силу своей ценности защищена не только с помощью системы нормативно-правовых актов, регулирующих процесс защиты такой информации и ответственность за незаконное завладение ей, но и сами хозяйствующие субъекты должны создавать надежные механизмы защиты информации от ее утечки [2].

У каждой корпорации или же в рамках государственных структур есть та информация, которая представляет особую ценность для таких учреждений. Такая информация, как правило, имеет закрытий характер и зачастую составляет коммерческую или государственную тайну. Таким образом, документация, содержащая подобную информацию, носит секретный или несекретный характер. Для того, чтобы документ имел секретность, он должен соответствовать критерию принадлежности информации, которая составляет государственную тайну, охраняемую норма-

ми действующего законодательства. Служебная же информация, составляющая коммерческую тайну (банковскую, производственную и т. д.) подпадает под категорией несекретной информации.

В целом под информацией принято понимать некие сведения о лицах, или же предметах, событиях и явлениях, представляемые в самом разнообразном виде [1].

Необходимо отметить, что информация, отраженная документально, признается нормами права на территории российского государства общедоступной, за исключением случаев, предусмотренных законодательством.

Классифицировать информацию можно на следующие категории:

1. Открытая информация, предназначенная и доступная для общего пользования.

2. Служебная информация, которая предназначена для использования внутри корпорации для служебных целей.

3. Секретная информация, предназначенная для ее использования ограниченным кругом лиц [3].

Второй и третий вид информации принято считать конфиденциальной.

Регулирование условий, которые выступают критериями конфиденциальности информации, происходит посредством статьи 13 Гражданского кодекса России. Таковыми условиями в силу закона являются:

1. Действительность информации, неизвестная третьим лицам.

2. Закрытый (ограниченный) доступ к информации в силу законодательно установленных ограничений.

3. Содействтие охране закрытой информации в рамках закона.

Таким образом, можно сделать вывод о том, что обеспечение секретности информации рассматривается через следующие аспекты такой информации:

1. Установление информации, которая носит ограниченный характер своего распространения.

2. Установление круга лиц, которые будут иметь доступ к конфиденциальной информации.

3. Разработка системы документального оформления порядка работы с документацией закрытого типа [4].

Если все подобные аспекты не будут учтены, то в случае разглашения подобной информации сотрудника, который разгласил такие сведения, нельзя будет привлечь к ответственности.

Необходимо отметить, что в силу правовых норм, не каждая информация может носить конфиденциальный характер, то есть представлять некую ценность для третьих лиц, которая впоследствии может нанести урон или ущерб корпорации при распространении такой информации. Так, конфиденциальной информацией не признается лицензия на занятие какой-либо предпринимательской деятельностью. Уставные документы предприятия также не представляют собой ценной информации, которая могла бы представлять собой конфиденциальную информацию. Также не признаются конфиденциальными сведения об уплате налоговых платежей и т. д.

Необходимо отметить, что ценность информации может носить материальный характер, то есть иметь стоимость. При разглашении конфиденциальной информации предприятию может быть нанесен определенный ущерб в размере вполне конкретных убытков. Также ценность информации может заключаться в ее научном, технологическом или техническом значении.

Информация, имеющая ценность, подпадает под регулирование нормами патентного, авторского, смежных прав.

Отметим также в рамках настоящего исследования, что ценность информации – категория временная. Как правило, это определяется временем, которым обладает предприятие-конкурент для создания аналогичной информации.

Существует несколько каналов, по которым передается информация, в том числе и носящая закрытый характер. Например, каналы распространения информации могут быть деловыми, торговыми, техническими, через информационные сети и т. д.

Сам канал распространения информации представляет собой путь перемещения информации от одного источника к другому в силу определённых закономерностей и на легитимных началах. Если же информация передается без ведома заинтересованных лиц, происходит так называемая утечка информации.

Под утечкой информации конфиденциального характера принято понимать незаконный выход информации за пределы зоны защиты такой информации [4].

Возможность утечки информации закрытого типа указывает на уязвимость информации, что предполагает принятие мер по ее защите. Уязвимость информации может проявляться в виде хищения носителя информации (бумажного, электронного), утрата носителя информации, несанкционированное уничтожение информации, разглашение информации закрытого типа и т. д. В последние годы кибератаки с целью похищения информации стали все более набирать обороты. Также уязвимость информации может проявляться через разрушение информации, через ее блокирование и т.д. Как правило, уязвимой информация становится вследствие случайных или преднамеренных действий в отношении конфиденциальной информации. Уязвимой информацию могут сделать как сами люди, так и средства передачи информации, стихийные бедствия, технические средств обработки информации и т. д.

Следует разграничить понятия «утрата» и «утечка» информации. К утрате информации конфиденциального характера приводит ее хищение, утрата самого носителя информации, незаконное уничтожение носителя с информацией, искажение или блокирование информации. Что же касается утечки конфиденциальной информации, то к ней приводит именно само разглашение информации подобного характера [2].

Информация конфиденциального характера не может существовать самостоятельно. Она находит свое отражение на самых разных носителях, с помощью которых осуществляется ее сохранение, накопление, а также передача. Таким образом, происходит процесс использования информации.

Под носителем информации принято подразумевать физическое лицо или же материальный объект, с помощью которых информация находит свое отражение в виде преобразованных символов, сигналов, технических процессов и решений. Материальных объектов в настоящее время множество. Ими могут быть бумажные носители, магнитные ленты, пленки, диски, фотопродукция и т. д.

К основным каналам утечки информации конфиденциального характера можно отнести речевые каналы, физические и технические каналы.

Под речевым каналом принято понимать передачу информации от человека, владеющего ей, к лицу, заинтересованному в получении такой информации.

Под физическим каналом утечки принято понимать передачу информации конфиденциального характера от носителя к объекту, который имеет интерес к данной информации.

Технический канал утечки информации предполагает, что информация конфиденциального характера передается посредством различных технических устройств.

Также необходимо отметить, что на лицо, обладающее закрытым типом информации, может оказываться открытое (непосредственный контакт) или скрытое (опосредованное) воздействие с целью завладения информацией такого характера. К открытым средствам утечки информации можно отнести телефонные, мобильные системы, ресурсы сети Интернет и т. д. К скрытым же принято относить прослушивание с использованием специальных технических устройств, незаконный доступ к компьютеру и его данным, содержащим конфиденциальную информацию и т. д.

Получение информации третьими лицами явление частое. Как правило, третьи лица завладевают информацией вследствие утраты, неправильного уничтожения информации, пренебрежения средствами защиты информации, излишняя болтливость лица, владеющего информацией конфиденциального характера и т. д.

Утечка информации, представляющей для предприятия высокую ценность, может проходить по организационным каналам, которые достаточно разнообразны. Таким каналами могут стать [1]:

– трудоустроенные на предприятие лица, у которых появляется в силу должностных обязанностей доступ к такой информации;

– использование мошеннических способов заполучения необходимой информации посредством использования клиентов предприятия, партнеров и т. д.;

– соучастники, являющиеся работниками предприятия и т. д.

Таким образом, информация, являющаяся особенно важной для предприятия, может стать объектом мошеннических действий с целью ее завладения и последующего использования в собственных целях. Ввиду такой ситуации предприятия должны предпринять все необходимые меры по защите информации такого характера.

СПИСОК ЛИТЕРАТУРЫ

1. Аверченков, В. И. Аудит информационной безопасности : учеб. пособие / В. И. Аверченков. – М. : Флинта, 2021. – 679 с.

2. Бабаш, А. В. Информационная безопасность / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – М. : КноРус, 2021. – 136 с.

3. Баранова, Е. Информационная безопасность. Практикум / Е. Баранова. – М. : КноРус, 2019. – 328 с.

4. Вострецова, Е. В. Основы информационной безопасности : учеб. пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.

REFERENCES

1. Averchenkov V.I. *Audit informacionnoj bezopasnosti: ucheb. posobie* [Information Security Audit. Study Guide]. Moscow, Flint Publ., 2021. 679 p.

2. Babash A.V., Baranova E.K., Melnikov Yu.N. *Informacionnaja bezopasnost* [Information Security]. Moscow, KnoRus Publ., 2021. 136 p.

3. Baranova E. *Informacionnaja bezopasnost. Praktikum* [Information Security. Practicum]. Moscow, KnoRus Publ., 2019. 328 p.

4. Vostretsova E.V. *Osnovy informacionnoj bezopasnosti: ucheb. posobie dlja studentov vuzov* [Fundamentals of Information Security. Textbook for University Students]. Yekaterinburg, Izd-vo Ural. un-ta, 2019. 204 p.

FUNDAMENTALS OF INFORMATION SECURITY AND INFORMATION PROTECTION

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Information Security
Volgograd State University
yarikov.vladislav@volsu.ru
Prosp. Universitetskiy, 100, 400062 Volgograd, Russian Federation

Maxim V. Pashkov

Student, Department of Information Security,
Volgograd State University
IBm-221_992475@volsu.ru
Prosp. Universitetskiy, 100, 400062 Volgograd, Russian Federation

Abstract. The text deals with the protection of confidential information in enterprises and corporations. It describes the value of such information and the need to protect it from leaks and illegal encroachments. It discusses the role of regulations and the creation of information protection mechanisms by enterprises themselves. Information of particular value to corporations and government agencies and the secrecy status of documents containing such information are also discussed.

In addition to discussing the protection of confidential information, the article considers issues related to determining the value of information and its legal status. It is noted that not all information may be confidential or of value to third parties. It is defined that the value ofinformation can be material, scientific, technological or technical. The regulation of information by the norms of patent and copyright law is discussed. The temporal nature of the value

of information and its dependence on the time a competitor has to create similar information are emphasised. Different channels of information transmission, including classified information, are considered.

The paper also discusses the various channels of leakage of sensitive information, such as speech, physical and technical.

The authors discuss overt and covert methods of obtaining information as well as the causes of information disclosure, such as loss, improper destruction, a lack of attention to information protection and excessive talkativeness.

Key words: protection, system, security, information, technology.