Organizational tools protection as an element of general information protection system

Dombrovskaya L.[1], Vasyutina T.[2] (Russian Federation)

Организационные средства защиты информации как элемент общей системы защиты информации

Домбровская Л. А.[1], Васютина Т. Л.[2] (Российская Федерация)

[1]Домбровская Лариса Александровна / Dombrovskaya Larisa – кандидат педагогических наук, доцент;
[2]Васютина Татьяна Львовна / Vasyutina Tatiyana – кандидат технических наук, доцент,
кафедра математики и информатики,
Санкт-Петербургский университет МВД России, г. Санкт-Петербург

Аннотация: *в статье рассмотрены источники конфиденциальной информации и каналы ее утечки. Определены основные направления защиты информации, где наряду с организационной выделяют правовую и инженерно-техническую защиту информации.*
Abstract: *the article describes the sources of confidential information and channels of its leakage. Defined the main directions of information security, where along with the organizational secrete the legal and engineering and technical protection of information.*

Ключевые слова: *информационная безопасность, управление доступом, конфиденциальное делопроизводство, обеспечение конфиденциальности информации.*
Keywords: *information security, access control, confidential paperwork, ensuring the confidentiality of information.*

Для наиболее полного и глубокого анализа происходящих в сфере защиты конфиденциальной информации процессов, понимания сущности планируемых и проводимых в этих целях мероприятий, прежде всего, необходимо рассмотреть одно из важнейших направлений защиты конфиденциальной информации – организационную защиту информации[1].

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата [1].

Прежде чем перейти к определению организационной защиты, ее направлений и условий, рассмотрим источники конфиденциальной информации и каналы ее утечки.

Основными источниками конфиденциальной информации являются:

- персонал предприятия, допущенный к конфиденциальной информации;
- носители конфиденциальной информации (документы, изделия);
- технические средства, предназначенные для хранения и обработки информации;
- средства коммуникации, используемые в целях передачи информации;
- передаваемые по каналам связи сообщения, содержащие конфиденциальную информацию.

Способы обмена конфиденциальной информацией (например, между сотрудниками предприятия) могут носить как непосредственный (личный) характер, так и характер передачи формируемых на основе информации сообщений посредством технических средств и средств коммуникаций (различных средств и систем связи).

Из существующих способов обмена конфиденциальной информацией необходимо выделить *организационные каналы передачи и обмена информацией:*

- конфиденциальное делопроизводство (защищенный документооборот);
- совместные работы, выполняемые предприятием по направлениям его основной и иной деятельности;
- совещания (конференции), в ходе которых обсуждаются вопросы конфиденциального характера;
- рекламная и издательская (публикаторская) деятельность;
- различные мероприятия в области сотрудничества с иностранными государствами (их

[1] Основные методы и средства защиты информации в информационных системах наряду с организационными мерами рассмотрены в статье «Современные подходы к защите информации, методы, средства и инструменты защиты»

представителями и организациями), связанные с обменом информацией;

- научные исследования, деятельность диссертационных и иных советов учреждений и организаций;
- передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

Организационные каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты негативному воздействию со стороны злоумышленников, направленному на получение этой информации. Данное воздействие, в свою очередь, может привести к возникновению каналов утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на недопущение ее утечки и несанкционированного распространения (утраты носителей конфиденциальной информации).

Для определения необходимых мер по защите информации, необходимо провести классификацию всех возможных каналов утечки информации в зависимости от направлений и специфики деятельности предприятия, видов конфиденциальной информации, особенностей функционирования системы защиты информации и иных факторов.

Организационные каналы утечки конфиденциальной информации, возникающие в процессе деятельности предприятия, можно подразделить следующим образом [2]:

- по источникам угроз защищаемой информации (внешние и внутренние);
- по видам конфиденциальной информации или тайн (государственная, коммерческая, служебная или иная тайна; персональные данные сотрудников предприятия);
- по источникам конфиденциальной информации (персонал, носители информации, технические средства хранения и обработки информации, средства коммуникации, передаваемые или принимаемые сообщения и т.п.);
- по способам или средствам доступа к защищаемой информации (применение технических средств, непосредственная и целее направленная работа с персоналом предприятия, осуществление непосредственного доступа к информации, получение доступа к защищаемой информации агентурным путем);
- по характеру взаимодействия с партнерами (каналы утечки, возникающие в отсутствие взаимодействия, при осуществлении взаимодействия, в условиях конкурентной борьбы);
- по продолжительности или времени действия (каналы утечки постоянного, кратковременного, а также периодического или эпизодического действия);
- по направлениям деятельности предприятия (каналы утечки, возникающие в обычных условиях или при повседневной деятельности предприятия, при выполнении совместных работ, осуществлении международного сотрудничества, проведении совещаний, выезде персонала за границу, в ходе рекламной и публикаторской или издательской деятельности, при проведении научных исследований или командировании сотрудников предприятия);
- по причинам возникновения каналов утечки информации (действия злоумышленников, ошибки персонала, разглашение конфиденциальной информации, случайные обстоятельства).

Далее по тексту термин «защита информации» распространяется только на информацию, в установленном порядке отнесенную к конфиденциальной информации, если иное не оговорено особо:

- по каналам коммуникации, используемым для передачи, приема или обработки конфиденциальной информации (каналы утечки, возникающие при хранении, приеме-передаче, обработке или преобразовании информации, а также в канале связи, по которому передается информация);
- по месту возникновения каналов утечки информации (каналы утечки, возникающие за пределами территории предприятия или на территории предприятия – в служебных помещениях, на объектах информатизации, объектах связи и в других местах);
- по используемым способам и методам защиты информации (каналы утечки, возникающие при нарушении установленных требований по порядку отнесения информации к категории конфиденциальной, обращения с носителями информации, ограничения круга допускаемых к информации лиц, непосредственного доступа к информации персонала предприятия или командированных лиц, а также по причине нарушения требований пропускного или внутри объектового режимов).

Задачи по исключению возможных каналов утечки конфиденциальной информации решаются как отдельными должностными лицами (персоналом), так и структурными подразделениями предприятия, создаваемыми и функционирующими по различным направлениям защиты информации. Успешное решение этих задач невозможно без применения совокупности средств и методов защиты информации [3].

Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации. Однако организационной защите информации среди этих направлений отводится особое место.

Организационная защита информации призвана посредством выбора конкретных сил и средств, в том числе правовых и инженерно-технических, реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке.

Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности, осуществляемой руководителем предприятия в этой области, являются: планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций, распределение обязанностей и задач между должностными лицами и структурными подразделениями, аналитическая работа и т.д. Цель принимаемых руководством предприятия и должностными лицами организационных мер - исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите. Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

В нормативной и научной литературе используются два примерно равнозначных определения организационной защиты информации.

Организационная защита информации – составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии – регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе – раскрывает ее структуру на уровне предприятия. Вместе с тем оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

Основные направления организационной защиты информации [4, 5, 6]:

1. Организация допуска и доступа к конфиденциальной информации и документам.
2. Организация работы с носителями сведений.
3. Организация внутриобъектового и пропускного режимов и охраны;
4. Организация работы с персоналом.
5. Комплексное планирование мероприятий по защите информации.
6. Организация аналитической работы по предупреждению утечки конфиденциальной информации и контроля ее осуществления.

Построение системы организационной защиты информации должно базироваться на следующих принципах:

- *принцип комплексного подхода* – эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач, в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- *принцип оперативности принятия управленческих решений* (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации; данный принцип направлен, в том числе, и на упреждение предполагаемых угроз целостности конфиденциальной информации);

- *принцип персональной ответственности* – наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа функционирования системы защиты информации, в целях принятия своевременных мер по повышению ее эффективности;

- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Литература

1. *Парфенов Н. П., Стахно Р. Е.* Технология защиты персональных данных // Наука, техника и образование, 2016. № 4.
2. *Стахно Р. Е., Гончар А. А.* Защита информации в современном документообороте // Наука, техника и образование, 2016. № 4.
3. *Домбровская Л. А., Яковлева Н. А., Стахно Р. Е.* Современные подходы к защите информации, методы, средства и инструменты защиты // Наука, техника и образование, 2016. № 4.
4. Сайт Безопасник. [Электронный ресурс]. Режим доступа: http://www.bezopasnik.org2 (дата обращения: 27.10.2016).
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. Режим доступа: http://www.consultant.ru (дата обращения: 27.10.2016).
6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015). [Электронный ресурс]. Режим доступа: http://www.consultant.ru (дата обращения: 27.10.2016).