Как видно из таблицы, наибольшие затраты связаны с персоналом.

На основе полученных результатов осуществляется подбор наиболее действенных способов и средств защиты. Выбор конкретного варианта защиты проводится с учетом критерия эффективность/стоимость. Проверка эффективности системы защиты должна носить периодический характер и включать оценку актуальности и полноты положений установленной политики безопасности.

Таким образом, рассмотренная методика (ТСО) может дополнительно включать и другие традиционные способы оценки эффективности, такие как скрытые и открытые проверки. Скрытыми проверками могут быть электронные письма с использованием методов социальной инженерии или мониторинг действий пользователей; открытыми – проведение тестирования, внешнего или внутреннего аудита. Однако, в целом, рассмотренная методика и её приложение на определение эффективности информационной защиты финансово-кредитного органа позволяет выявить наиболее приемлемый вариант использования собственных информационных ресурсов и обеспечения безопасной работы с коммерческой информацией.

**Литература:**

1. Киселев В.Д., Есиков О.В., Кислицын А.С. *Современные проблемы защиты в системах ее передачи и обработки* / Под ред. проф. Е.М. Сухарева. – М.: изд. «Солид», 2006. – С.200.
2. Середа С. *Программно-аппаратные системы защиты программного обеспечения*. – СПб.: Издательство BHV-Петербург, 2006. – 320 с.
3. http://www.it.ru – сайт компании АйТи.
4. http://bezpeka.com/ – оценка эффективности систем защиты информации.

***Денис Евтодиенко,***
*Министерство информационного развития*

# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

В связи со стремительным развитием информационных технологий в настоящее время защита персональных данных стала важным и актуальным вопросом для всех организаций. Персональные данные есть в отделе кадров, в бухгалтерии и даже в отделе продаж, что требует их защиты.

В связи с этим к персональным данным предъявляются основные требования информационной безопасности, такие как обеспечение целостности, доступности и конфиденциальности данных. Защита персональных данных должна достигаться путем исключения несанкциониро-

ванного доступа к персональным данным, в результате которого возможны уничтожение, модификация, копирование, распространение персональных данных и другие несанкционированные действия [1].

Среди основных принципов организации автоматизированной обработки персональных данных можно выделить:

- персональные данные должны быть собраны только для определенных целей и в строгом соответствии с действующим законодательством;
- персональные данные должны быть точными, полными и своевременно обновленными;
- цели, для достижения которых собираются и обрабатываются персональные данные, должны быть определены и утверждены до начала деятельности и использоваться только в этих целях;
- должна быть внедрена система защиты персональных данных;
- деятельность организаций (как государственных, так и частных), являющихся держателями персональных данных, должна быть открытой для заинтересованных лиц и контролирующих органов;
- необходимо создание независимого контролируемого органа как важного элемента защиты персональных данных.

Система защиты персональных данных при их обработке в информационных системах должна выполнять следующие задачи:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным;
- своевременное обнаружение фактов, событий несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование;
- незамедлительное восстановление модифицированных или уничтоженных персональных данных;
- постоянный контроль над обеспечением уровня защищенности персональных данных.

Организации, осуществляющие деятельность, связанную с обработкой персональных данных, должны обеспечивать защиту персональных данных, применяя основные меры и средства обеспечения безопасности:

- организационные меры защиты информации;
- средства предотвращения несанкционированного доступа, утечки информации по техническим каналам;
- криптографические средства защиты информации;
- средства предотвращения программно-технических воздействий на технические средства обработки персональных данных и другие.

Все технические, программные и организационные меры и средства защиты персональных данных

должны удовлетворять требованиям и положениям действующего законодательства и должны проходить процедуру оценки соответствия.

В соответствии с Законом Республики Молдова «О защите персональных данных» уполномоченный Национальный центр по защите персональных данных имеет право возлагать на организации дополнительные обязанности по обеспечению безопасности персональных данных при их обработке.

В связи с усложнением топологии сетей из-за использования дополнительных средств обеспечения безопасности существенно увеличиваются операционные и технологические риски. Также появились новые группы рисков, такие как государственные и правовые, связанные с возможными санкциями Национального центра по защите персональных данных за невыполнение требований закона Республики Молдова «О защите персональных данных», а также с исками субъектов персональных данных.

Таким образом, требования к системе защиты персональных данных должны определяться в зависимости от объема и категории обрабатываемых персональных данных.

Среди основных действий, необходимых для управления системой защиты персональных данных при их обработке в информационных системах организаций, можно выделить [3]:

- определение угроз и уязвимостей безопасности, направленных на персональные данные при их обработке;
- формирование модели нарушителей как внутренних, так и внешних, на основе выявленных угроз и уязвимостей;
- разработка системы защиты персональных данных, обеспечивающей минимизацию выявленных угроз с использованием различных методов и способов защиты персональных данных;
- тестирование готовности средств защиты информации;
- внедрение и ввод в эксплуатацию средств защиты информации;
- обучение персонала, использующего средства защиты информации, применяемые в информационных системах;
- учет используемых средств защиты информации, документации к ним, носителей персональных данных;
- учет ответственных лиц, допущенных к работе с персональными данными в информационной системе;
- периодический контроль над использованием средств защиты персональных данных.

Следует отметить актуальность вопроса о предоставлении персональных данных третьим сторонам как с точки зрения наличия основания для предоставления данных, так и с точки зрения обязательного наличия договора с данной стороной, в котором должна быть установлена обязанность обеспечения конфиденциальности и безопасности персональных данных третьей стороной.

В заключение можно отметить основные проблемы в области защиты персональных данных, такие

как высокая сложность и, соответственно, стоимость работ по защите персональных данных, а также понимание установленных требований защиты. Исходя из существующих проблем в данной области, необходимо обеспечить, чтобы работы по защите персональных данных при их обработке в информационных системах были неотъемлемой частью работ по созданию самих информационных систем.

**Список нормативной и научной литературы:**

1. Закон Республики Молдова «О защите персональных данных» №17 от 15.02.2007.
2. Закон Республики Молдова «Об утверждении Положения о Национальном центре по защите персональных данных, структуры, предельной штатной численности и порядка финансирования» №182 от 10.07.2008.
3. www.itsec.ru.

***Александр Жека,*** *«INTEXNAUCA" S.A.*

# АУДИТ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

*The art of information security auditing is not only a measurement of the quality of technical means of protection, but also in evaluating the quality of their service and level of business process organization. Key indicators should describe the status of all properties of the object, because this is the only way to make the right conclusion about the state of information security in the organization.*

Важнейший ресурс современного общества – информация – одновременно несет в себе и огромную угрозу для него, связанную с внутренней спецификой этого ресурса. Простота и большое число различных способов доступа и модификации информации, значительное количество квалифицированных специалистов, широкое использование в общественном производстве специальных технических средств позволяют злоумышленнику практически в любой момент и в любом месте осуществлять действия, представляющие угрозу информационной безопасности как в локальном, так и в глобальном масштабах.

Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с определенными критериями информационной безопасности.

Основная задача аудита – объективно оценить текущее состоя-