# Политика безопасности для программы бухгалтерского отчета

*Выполнил студент ПК-12-2 Бекленищев Влад*

## Описание объекта защиты

Программа бухгалтерского учета (или просто бухгалтерская система) - это система автоматизации, которая позволяет вести как бухгалтерский так и фискальный (тот, который направленный на удовлетворение требований государства по расчёту и уплате налогов) учет.

Основными объектами защиты системы информационной безопасности в программе бухгалтерского учета являются:

* информационные ресурсы, содержащие информацию о расчетах, прибыли, убытках;
* информационные ресурсы, содержащие данные о поставках и поставщиках
* информационные ресурсы, содержащие данные о платежах, состояний платежей и их истории;

## Цели и задачи деятельности по обеспечению информационной безопасности

Целью деятельности по обеспечению информационной безопасности программы бухгалтерского учета является снижение угроз информационной безопасности до приемлемого для программы бухгалтерского учета уровня.

Основные задачи деятельности по обеспечению информационной безопасности в программе бухгалтерского учета:

* выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* предотвращение инцидентов информационной безопасности;
* исключение либо минимизация выявленных угроз.

## Угрозы информационной безопасности

Возможны такие угрозы в программе бухгалтерского учета:

* несанкционированный доступ к системе в лице других сотрудников или посторонних личностей;
* отсутствие контроля ввода данных. В таком случае даже сам абонент системы может сделать ошибку ввода из-за чего появится совсем иной результат.
* отсутствие контроля и фиксирования изменений в системе программного обеспечения. Имеется в виду изменение конфигурации такого ПО;
* вирусное ПО, которое может осуществлять все выше перечисленные угрозы, а также полное уничтожение системы.
* возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, не обусловленных деятельностью человека.
* возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

## Модель нарушителя информационной безопасности

Нарушителями для программы бухгалтерского учета могут являться следующие личности:

* зарегистрированные пользователи системы имеющие полный или частичный доступ к системе;
* сотрудники предприятия не имеющие доступ к системе;
* персонал, обслуживающий технические средства, на которых установлена программа бухгалтерского учета;
* сотрудники, задействованные в разработке и в сопровождение программного обеспечения;
* посетители зданий и помещений предприятия;
* лица, случайно или умышленно проникшие в корпоративную информационную систему предприятия из внешних телекоммуникационных сетей (хакеры).

## Основные положения по обеспечению информационной безопасности

Можно выделить следующие основные положения и требования по обеспечению безопасности бухгалтерской системы:

* Требования об обеспечении информационной безопасности бухгалтерской системы обязательны к соблюдению всеми работниками предприятия и пользователями информационных систем.
* Неисполнение или некачественное исполнение сотрудниками и пользователей бухгалтерской системы обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к системе, а также применение к виновным административных мер воздействия, степень которых определяется установленным в предприятии порядком либо требованиями действующего законодательства.
* Ограничение доступа к вычислительной системе через регистрацию. В этом случае после процесса аутентификации система сможет авторизовать пользователя предоставив ему полный или частичный доступ.
* Выполнение тестирования и верификации изменений в системе программного обеспечения и программах защиты.
* Осуществление контроля за изменениями в системе бухгалтерского учета. Таким образом, можно избежать ошибок, которые могли допустить сотрудники имеющие доступ к системе.
* Установление ограничений в привилегиях персонала, обслуживающего СОД (система обработки данных) выполнение гарантийных требований в случае нарушений;
* Проведение записей протокола о доступе к системе, а также компетентности обслуживающего персонала.

Менеджмент инцидентов информационной безопасности, включающий:

* сбор информации о событиях информационной безопасности;
* выявление и анализ инцидентов информационной безопасности;
* расследование инцидентов информационной безопасности;
* оперативное реагирование на инцидент информационной безопасности;
* минимизация негативных последствий инцидентов информационной безопасности.

## Организационная основа деятельности по обеспечению информационной безопасности

В целях выполнения задач по обеспечению информационной безопасности системы бухгалтерского учета должны быть определены следующие роли:

* Ответственное подразделение;
* Сотрудники предприятия:

При необходимости могут быть определены и другие роли по информационной безопасности.

Задачами **ответственного подразделения** являются:

* разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности предприятия, включая планы, политики, положения.
* обучение, контроль и непосредственная работа с персоналом Банка в области обеспечения информационной безопасности;
* планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Банке;
* выявление и предотвращение реализации угроз информационной безопасности;
* выявление и реагирование на инциденты информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности;
* пресечение несанкционированных действий нарушителей информационной безопасности;
* разработка оптимальных процедур реагирования на инциденты и обучение персонала;

## Резюме

В данной лабораторной работе производилась разработка политики безопасности для программы бухгалтерского учета. Для этого был произведен анализ уязвимых мест подобного ПО, а именно информационных, программных, материальных.

Исследовалось каким именно видам угроз может подвергаться система бухгалтерского учета, а также были приведены модели нарушителей для данной системы.

Исследования показали, что чаще всего программа бухгалтерского учета может подвергаться таким основным угрозам:

* отсутствие контроля ввода данных. В таком случае даже сам абонент системы может сделать ошибку ввода из-за чего появится совсем иной результат. Такая проблема является самой популярной угрозой.
* отсутствие контроля и фиксирования изменений в системе программного обеспечения. Имеется в виду отстутствие протоколирования всех изменений. В этом случае тяжело вычислить нарушитетеля системы.
* несанкционированный доступ к системе в лице других сотрудников или посторонних личностей. Для избежания такой угрозы есть авторизация пользователей, которая предоставляет либо частичный либо полный доступ.

После исследования угроз были предложены методы решения (в кратце описанные в основных угрозах выше) для защиты данной информации в качестве основных положений. Также были описаны основные задачи ответственного подразделения, которое поддерживает информационную безопасность.