# ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ ЦЕНТРОВ АВТОРИЗАЦИИ КАРТ ПЛАТЕЖНЫХ СИСТЕМ В ХОДЕ СОТРУДНИЧЕСТВА РОССИЙСКИХ И ЗАРУБЕЖНЫХ ВУЗОВ

**Кручинина С.А.,**
**Сухотерин А.И.**
Московский государственный областной технологический университет, Королев, Российская Федерация.

Наличие детально проработанной программы развития и интеграции всех составляющих инженерной инфраструктуры (информационных технологий, телекоммуникаций и защиты информации) современных центров авторизации платежных карт обуславливает их успешное развитие. Однако такое развитие информационных технологий предполагает значительные финансовые вложения в программно-аппаратные средства, в том числе выбор средств защиты информации, который во многом зависит от технологических возможностей применяемых программно-аппаратных средств.

Предложенный подход организации информационной безопасности может быть полезен при планировании поэтапного внедрения средств защиты информации, а также для повышения эффективности выполнения мер информационной безопасности, полноты и четкости предварительно проведенных организационных мероприятий, качества нормативных документов, планирования сроков проведения работ.

**Ключевые слова:** организация, защита информации, центр авторизации карт, платежная система.

# ORGANIZATION OF INFORMATION SECURITY IN PAYMENT CARD AUTHORIZATION CENTER IN THE PROCESS OF COOPERATION BETWEEN RUSSIAN AND FOREIGN UNIVERSITIES

**Kruchinina S.A.,**
**Sukhoterin A.I.**
University of Technology, Korolev, Russian Federation

The availability of a detailed program for the development and integration of all components of the engineering infrastructure (information technology, telecommunications and information protection) of modern payment card authorization centers determines their successful development. However, such development of information technologies implies significant financial investments in software and hardware, including the choice of

information protection tools, which largely depends on the technological capabilities of the software and hardware used.

The proposed approach to the organization of information security can be useful in planning the step-by-step introduction of information security tools, as well as to improve the effectiveness of the implementation of information security measures, completeness and clarity of pre-arranged organizational arrangements, the quality of regulatory documents, and the scheduling of work.

**Keywords:** organization, information security, card authorization center, payment system.

Успешное развитие современных информационных служб центров авторизации платежных карт (далее – ЦАПК) требует тщательно разработанной программы развития и интеграции всех составляющих их инженерной инфраструктуры: информационных технологий, телекоммуникаций и защиты информации.

Для реализации защиты информации предлагается разработать концепцию комплексной системы защиты информации и поэтапно выполнять комплекс мер по ее внедрению.

Развитие информационных технологий требует значительных финансовых вложений в программно-аппаратные средства. Учитывая, что в базах центров авторизации платежных карт содержится информация, полная или частичная потеря которой неизбежно приведет к значительным, а в ряде случаев невосполнимым финансовым потерям, которые могут быть выше, чем средства, потраченные на создание информационных служб, необходимо обеспечить надежную защиту всех компонентов центров авторизации.

Для создания системы защиты информации предлагается использовать комплексный подход, а именно: создание «Единого пространства информационной безопасности», как комплекса взаимосвязанных и постоянно взаимодействующих технических, организационных и нормативно-правовых подсистем. Необходимым условием функционирования таких подсистем является создание политики безопасности.

В соответствии с международными рекомендациями за безопасность работы всех служб центров авторизации должны отвечать сотрудники службы информационной безопасности, в обязанности которых входит круг вопросов связанных с обеспечением постоянного мониторинга состояния информационной безопасности (защиты информации), контроля привилегий и действий пользователей (рис. 1).

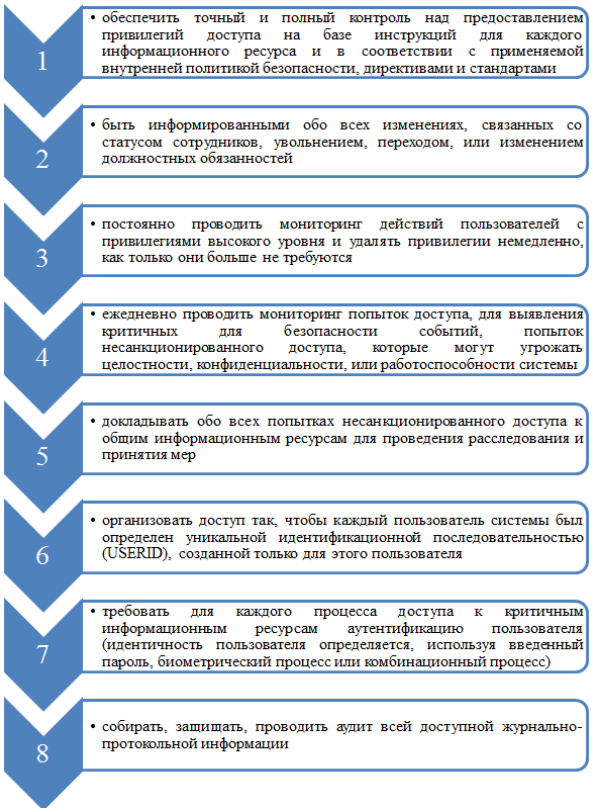


**Рисунок 1 – Обязанности специалистов по информационной безопасности**

Таким образом, на всех стадиях внедрения информационных технологий комплексно решается вопрос защиты информации, предоставляется подход для юридического решения споров между пользователями информационных технологий, разделение обязанностей между подразделениями, четко определяются границы ответственности между должностными лицами.

Цель информационной защиты – обеспечение надежной, корректной и безопасной работы всех компонентов ЦАПК, что подразумевает создание надежных и удобных механизмов регламента деятельности служб, пользователей и обслуживающего персонала, соблюдение дисциплины доступа к ресурсам информационной системы.

Для создания защиты информации информационных технологий ЦАПК необходимо использовать комплексный подход, а именно: создание защищенной среды для обработки информации, которая объединит разнообразные (правовые, организационные, программно-технические) средства для отражения любой угрозы.

При этом не следует забывать об особенностях информационных сетей (далее – ИС) ЦАПК, главной из которых является неоднородность их

компонентов, включая используемые операционные системы и прикладные программы (рис. 2):


**Рисунок 2 – Особенности информационных сетей ЦАПК**

1. Программно-аппаратными средствами для систем авторизации, клиринговых систем и систем мониторинга служат сервера баз данных (ORACLE и т.п.);
2. Многочисленные приложения на рабочих станциях в основном работают в операционной среде WINDOWS, но могут использоваться другие операционные системы (OS/2 и т.д.), терминалы, для файловых серверов могут применяться ОС WINDOWS-NT/2000, LINUX;
3. В качестве средств маршрутизации и коммутации чаще всего используются продукты CISCO, однако могут быть использованы продукты других фирм;
4. Взаимодействие служб ЦАПК осуществляется на базе TCP/IP протокола, используя сети компаний провайдеров телекоммуникационных услуг или выделенные каналы связи;
5. Подключение банкоматов осуществляется на базе протоколов TCP/IP и X.25, используя сети компаний провайдеров телекоммуникационных услуг или выделенные каналы связи;
6. Взаимодействие с сетью POS-терминалов реализуется через коммутируемые каналы связи;
7. Территориальная распределенность компонентов информационной сети, включая информационные ресурсы, необходимость взаимодействия с глобальными платежными системами VISA, EUROPAY и т.д. затрудняет организацию централизованного управления и мониторинга всех средств сети передачи данных.

По результатам анализа информационной системы распределенных информационных объектов интернет-банкинга как объекта

информационной безопасности были выявлены следующие наиболее опасные типы угроз (рис. 3):

- угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений;
- угрозы безопасности и работоспособности систем авторизации;
- угрозы безопасности и работоспособности телекоммуникационных средств.

Для создания эффективной системы противодействия перечисленным угрозам необходимо обеспечить совокупность программно-технических средств, организационных (административных) правил, правовых и морально-этичных норм.

На первом этапе необходимо реализовать комплексное управление доступом и защиту от несанкционированного доступа (далее – НСД) в информационной сети в целом, разработать и утвердить «Положение об информационной сети ЦАПК», структура которой представлена далее (рис. 4).


**Рис. 4 – Структура информационной сети ЦАПК**

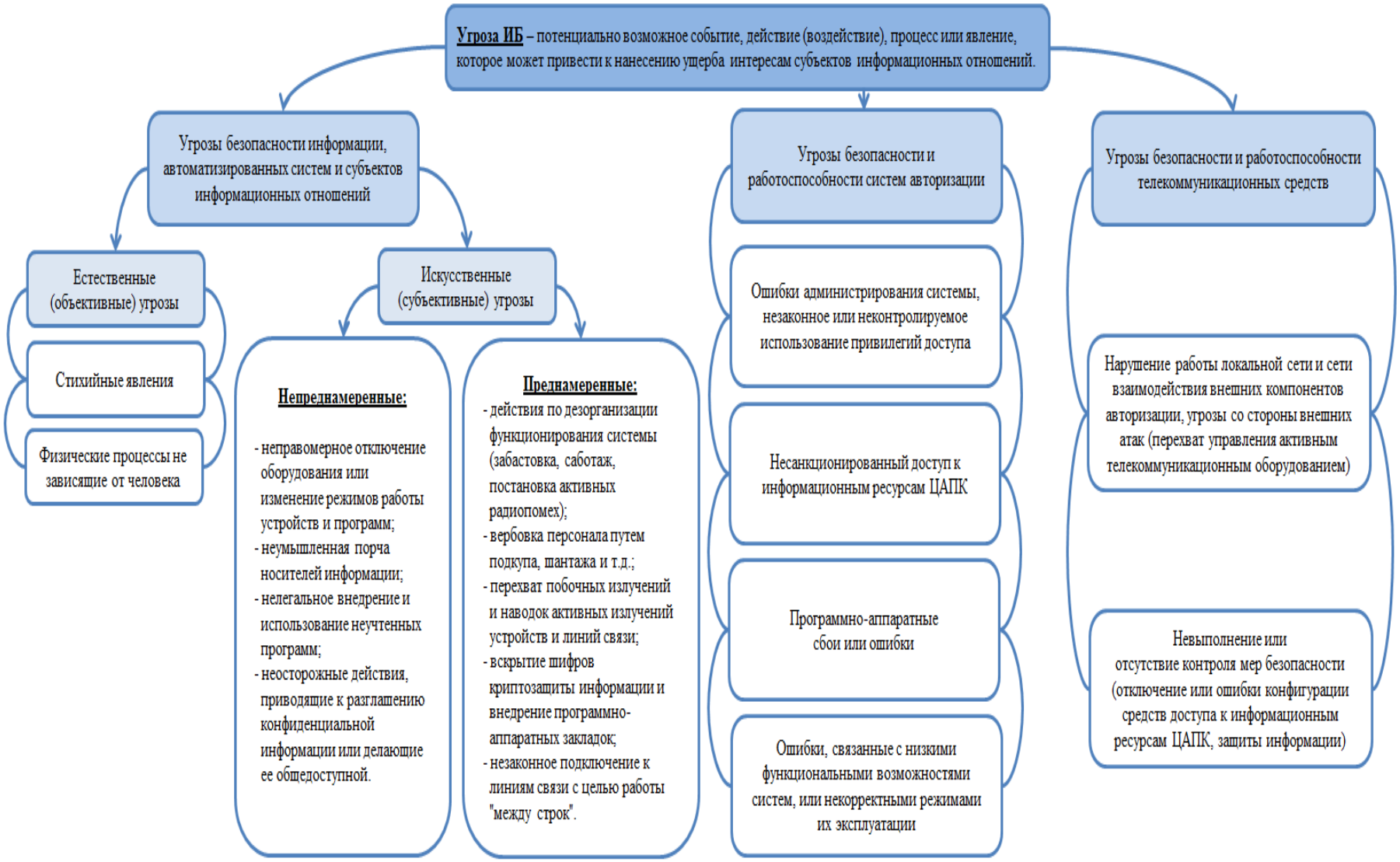


**Рисунок 3 – Наиболее опасные типы угроз информационной безопасности**

Необходимо обозначить основные информационные потоки между компонентами ЦАПК. Учитывая организационную структуру информационного объекта, для сотрудников и служб операционного, расчетного и технического отделов ЦАПК необходимо регламентировать процессы функционирования процессинговых систем, использование информационных ресурсов, деятельность сотрудников, включая доступ к информационным ресурсам.

В «Положении об информационной сети ЦАПК» необходимо отразить следующие ключевые положения (рис. 5):


**Рис. 5 – Положение об информационной сети ЦАПК**

На базе созданного Положения необходимо разработать и утвердить «Концепцию технической защиты информационной сети ЦАПК», при этом отделу информационной безопасности (защиты информации) целесообразно разработать и внедрить ряд нормативных документов, в которых необходимо закрепить следующие узловые моменты (рис. 6).

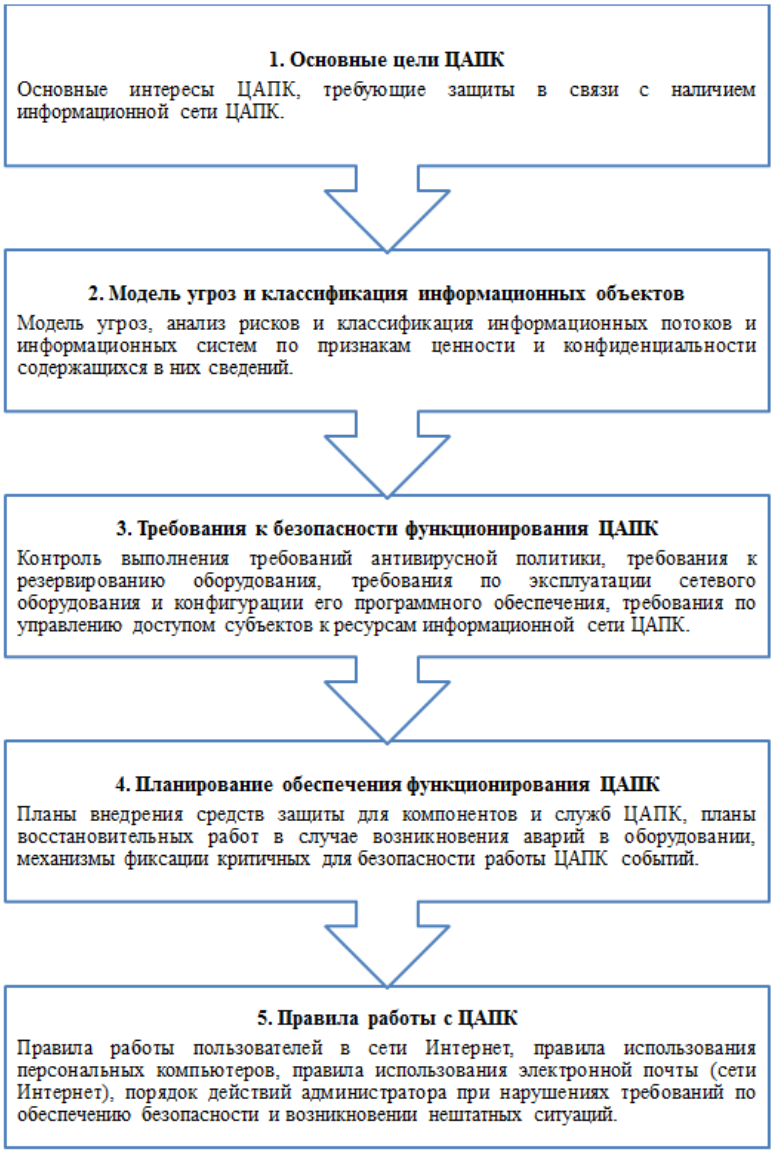


**Рис. 6 – Концепция технической защиты информационной сети ЦАПК**

Реализация предложенных мер требует создания комплексной системы защиты ИС ЦАПК (рис. 7).

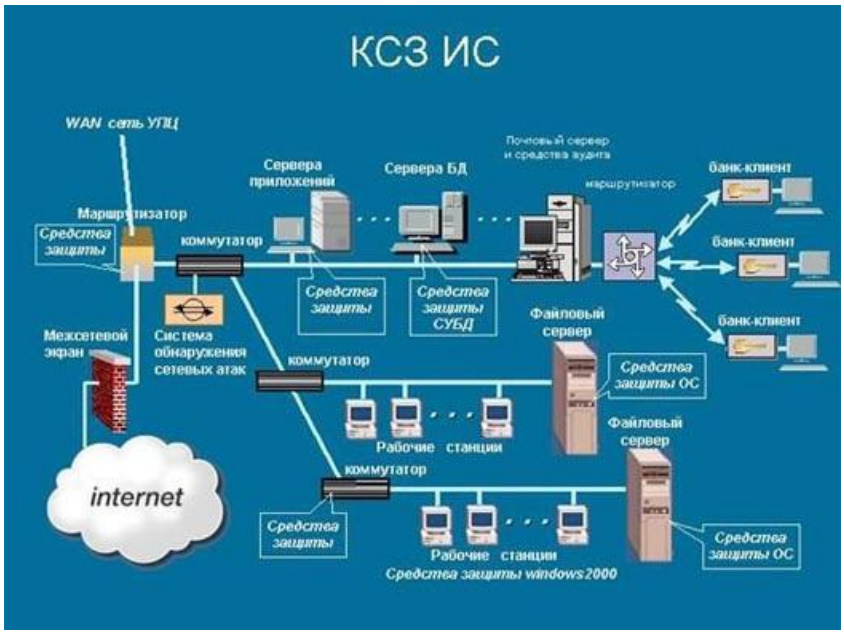


**Рис. 7 – Комплексная система защиты ИС ЦАПК**

При этом необходимо использование как штатных:

- криптографические средства, реализованные в платежных системах;
- средства разграничения доступа и криптографии, реализованные в ОС WINDOWS 2000;
- средства разграничения доступа ОС, реализованные в операционных системах файловых серверов;
- средства разграничения доступа, реализованные в СУБД;
- средства разграничения доступа, реализованные в устройствах коммутации пакетов;

так и дополнительных средств защиты:

- средства разграничения доступа, обнаружения сетевых атак и межсетевого экранирования, для устройств коммутации пакетов;
- средства защиты, реализованные для различных компонентов платежной системы ЦАПК (защищенная электронная почта и т.д.);
- средства защиты, реализованные в различных приложениях и комплексах ЦАПК;
- средства идентификации и аутентификации доступа к серверам приложений;
- средства мониторинга и контроля информационной сети ЦАПК.

Учитывая организационную структуру ЦАПК, а также структуру его взаимодействия с внешними компонентами, создание защищенной среды для обработки информации целесообразно начать с внедрения защищенной автоматизированной системы единого файлового обмена между информационными службами ЦАПК.

Имея единый защищенный файловый обмен между сотрудниками ЦАПК на базе правовых и морально-этичных норм, в должностные обязанности включаются права и ответственность за переданную и принятую информацию, внедряется контроль обмена между приложениями компонентов ЦАПК, организационными мерами обеспечиваются права и ответственность должностных лиц, ответственных за работу приложений. Каждый переданный файл должен иметь владельца (отправителя), ответственного за передаваемую информацию, подтвержденную его цифровой подписью, и механизмы, гарантирующие, что файл будет доставлен и принят только указанным получателем. На базе такой технологии будут строиться все правовые взаимоотношения между сотрудниками.

На втором этапе для каждой рабочей станции определяются ресурсы, нуждающиеся в защите, основные угрозы для различных информационных ресурсов и требования к защите от этих угроз. На рабочих местах и серверах ЦАПК средства защиты от НСД. Для этих целей на все рабочие станции ЦАПК устанавливается ОС WINDOWS 2000/XP, конфигурируются для каждой рабочей станции средства разграничения доступа и средства для аудита и контроля и т.д. Для файловых серверов, серверов баз данных, средств маршрутизации выбираются средства для организации разграничения доступа, аудита и контроля и т.д.

Со стороны службы информационной безопасности обеспечивается полный контроль соблюдения требований защиты от НСД, непрерывное выявление и регистрация внешних и внутренних умышленных и неумышленных, прямых и косвенных нарушений политики безопасности, имеющих как объективную, так и субъективную природу, с обеспечением администратору безопасности возможности доступа ко всей необходимой информации из одной точки.

Для реализации поставленной задачи целесообразно применять системы мониторинга и аудита средств защиты информационной сети. Наиболее предпочтительным вариантом является система централизованного мониторинга и аудита «Мираж» (рис. 8), разработчик ООО «Институт компьютерных технологий» г. Киев.

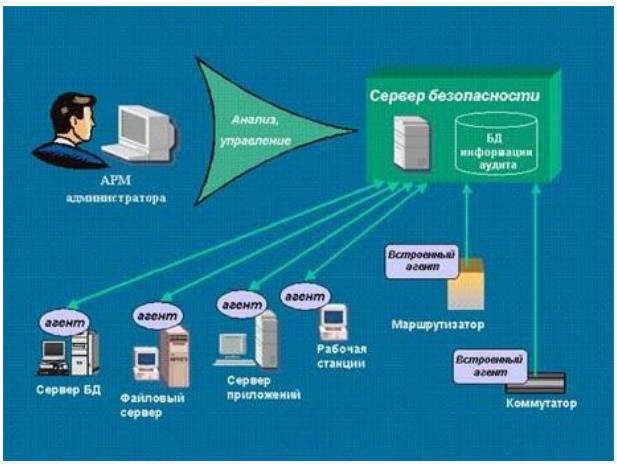


**Рис. 8 – Система «Мираж»**

Данная система обладает следующими функциональными возможностями:

- контроль действий администраторов по назначению полномочий по доступу к ресурсам ИС;
- контроль соответствия назначенных полномочий установленным правилам разграничения доступа;
- контроль событий, связанных с попытками НСД к ресурсам ИС;
- контроль событий, связанных с нарушением работоспособности компонентов ИС;
- анализ и обработка информации по заданным правилам в реальном времени;
- немедленное оповещение администратора безопасности обо всех выявленных нарушениях;
- ведение архивов зарегистрированных данных и данных аудита;
- подготовка сводных отчетов различной структуры.

Для каждого сотрудника, исходя из его должностных обязанностей, определяются правила разграничения доступа к информационным ресурсам. Внутренние нормативные документы ЦАПК, учитывая технологию обработки информации, определяют информационные ресурсы, нуждающиеся в защите, основные угрозы и требования к защите от этих угроз.

В целом политика безопасности определяется технологией обработки информации, особенностями используемых аппаратных и программных средств, физической средой, в которой эксплуатируется программно-аппаратные средства ЦАПК.

Как часть политики безопасности выступают регламентирующие правила доступа пользователей к информационным ресурсам, которые необходимо определить для каждого пользователя-сотрудника ЦАПК (рис. 9)

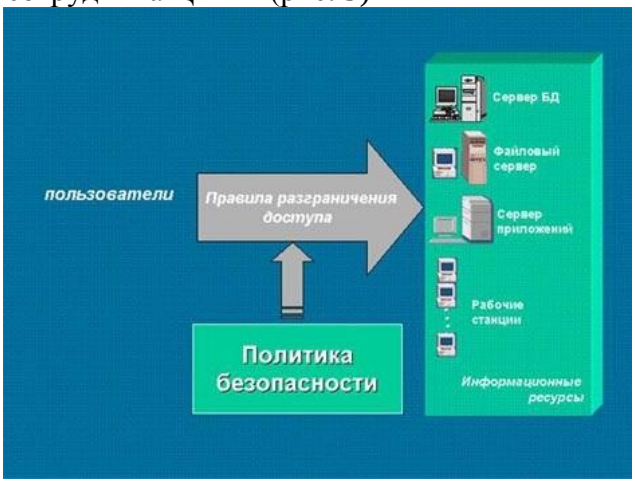


**Рис. 9 – Регламентирующие правила доступа**

Эффективность выполнения мер безопасности во многом зависит от полноты и четкости предварительно проведенных организационных мероприятий, качества нормативных документов, планирования сроков проведения работ, и т.д.

Для полного контроля, анализа и управления средствами защиты необходимо создать централизованную базу данных аудита. Сбор информации со всех установленных средств защиты осуществляет сервер безопасности путем взаимодействия со своими агентами, установленными на контролируемых объектах, с защищаемыми информационными ресурсами.

В зависимости от используемой системы авторизации ее отдельные компоненты и службы имеют средства контроля и диагностики технологических процессов. Для контроля в целом процесса авторизации на третьем этапе рекомендуется разработать и внедрить комплекс технологического контроля процессинговой системы.

Комплекс обеспечит контроль над работой системы авторизации, посредством анализа работы всех её компонентов на предмет корректной обработки транзакций. Комплекс должен контролировать достоверность, вырабатываемой компонентами системы информации, путем ведения достоверной единой базы обработки транзакций, содержащей данные с результатами поступивших и обработанных транзакций, а также иметь механизмы доступа и обработки данных существующих баз компонентов процессинговой системы (рис. 10).

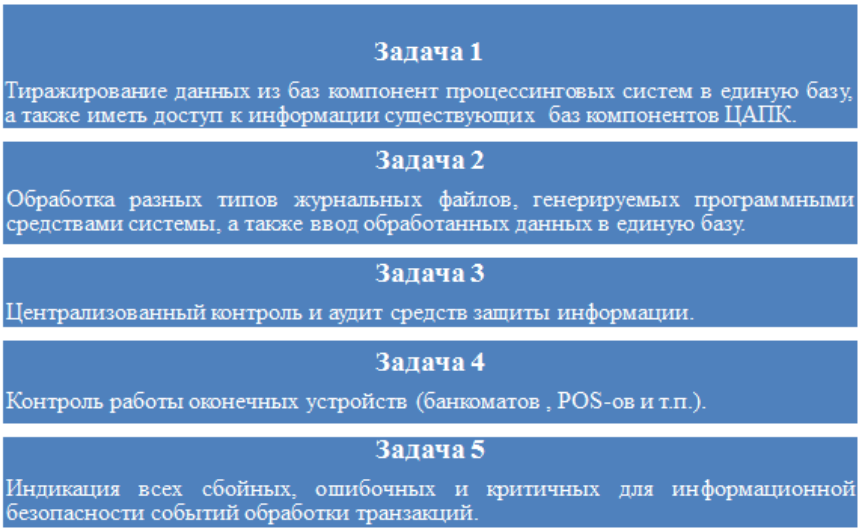


**Рис. 10 – Задачи комплекса технического контроля процессинговой системы**

Комплекс должен обеспечить централизованный анализ и управление, что в целом обеспечит устойчивую и безопасную работу всех компонентов информационной сети ЦАПК.

Таким образом, информационная система распределенных информационных объектов интернет-банкинга как объект информационной безопасности обладает следующими ключевыми характеристиками:

- одним из главных условий успешного развития современных ИС ЦАПК является наличие детально проработанной программы развития и интеграции всех составляющих ее инженерной инфраструктуры: информационных технологий, телекоммуникаций и защиты информации;
- развитие таких технологий требует значительных финансовых вложений в программно-аппаратные средства;
- в целях создания механизма защиты информации ИС ЦАПК необходимо применять комплексный подход, заключающийся в создании защищенной среды для обработки информации, которая объединит разнообразные (правовые, организационные, программно-технические) средства для отражения любой угрозы;
- выбор средств защиты информации во многом зависит от технологических возможностей применяемых программно-аппаратных средств, а эффективность

выполнения мер ИБ – от полноты и четкости предварительно проведенных организационных мероприятий, качества нормативных документов, планирования сроков проведения работ, и т.д.

*Литература*


1. Указ Президента Российской Федерации от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
2. Международный стандарт ISO/IEC 17799:2000 «Информационные технологии – практические правила управления информационной безопасностью»;
3. Международный стандарт ISO/IEC 27001:2013 «Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования»;
4. Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;
5. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 10.01.2016);
6. Информационная безопасность предприятия: Учебное пособие / Н. В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015;
7. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В. В. Чудовский. – М.: Издательский центр «Академия», 2009;
8. Сбербанк полностью перейдёт на бесконтактную оплату к 2020 году. Электронный ресурс. Режим доступа: http://www.3dnews.ru/940991 (дата обращения: 11.09.2017);
9. Национальное достояние: что делают с «Миром» россияне. Электронный ресурс. Режим доступа: www.banki.ru/mir/ (дата обращения: 18.09.2017)
10. Муки рождения российской НСПК. Электронный ресурс. Режим доступа: http://myfin.by/stati/view/3703-muki-rozhdeniya-rossijskoj-nspk-nastuplenie-kriptovalyut-i-smsoplata-parkovki (дата обращения: 23.09.2017).
11. Национальная система платежных карт (НСПК). Электронный ресурс. Режим доступа: http://www.tadviser.ru/index.phpКомпания: Национальная система платежных карт (НСПК) (дата обращения: 11.09.2017);
12. Банки и клиенты снова жалуются на сбои в работе НСПК. Электронный ресурс. Режим доступа: http://izvestia.ru/news/586227 (дата обращения: 23.09.2017);
13. «Мир» нашему дому, или рождение российской пластиковой карты. Электронный ресурс. Режим доступа: http://mircreditov.info/mir-nashemu-domu-ili-rozhdenie-rossijskoj-plastikovoj-karty.html (дата обращения: 18.09.2017);
14. Соляной В.Н., Сухотерин А.И, Шихнабиева Т.Ш., Сиротский А.А. Некоторые элементы ассоциативности в методиках преподавания дисциплин технической направленности. Организация менеджмента информационной безопасности в финансово-кредитных учреждениях. Информационная безопасность бизнеса и общества. Сборник статей научно - преподавательского состава кафедры информационных систем, сетей и безопасности / Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016.-111 с.;
15. Сухотерин А.И., Белов Д.С. Интеллектуализация управленческих процессов информационной безопасности на основе использования технологии слияния сенсорной информации. Научный журнал №2 (08) 2016г. Информационно-технологический вестник г. Москва. МО: Изд-во «Научный консультант», МГОТУ, 2016. с. 84-92 (120 с).