А. С. Зайцев

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВОЙ ОРГАНИЗАЦИИ С ПРИМЕНЕНИЕМ ПРОЦЕССОВ МОДЕЛИРОВАНИЯ, КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ АКТИВОВ И УЧЕТНЫХ ЗАПИСЕЙ

Кредитно-финансовая система Российской Федерации является, согласно Доктрине информационной безопасности Российской Федерации [1], одной из наиболее подверженных угрозам информационной безопасности (ИБ) систем страны, а обеспечение ИБ организации банковской системы РФ (БС РФ) играет ключевую роль в обеспечении ИБ РФ и национальной безопасности государства в целом.

Согласно стандарту Банка России [2], обеспечение ИБ организации БС РФ достигается путем проектирования, внедрения, анализа и совершенствования системы обеспечения информационной безопасности (СОИБ), состоящей из системы ИБ и системы менеджмента ИБ.

При этом СТО БР ИББС, как и его прообраз ISO 27001 [3], предлагает использовать процессный подход для менеджмента ИБ.

Одними из важнейших процессов ИБ являются процессы моделирования, классификации активов и учетных записей, которые и рассмотрены в настоящей статье.

Под объектом защиты в рамках настоящей статьи будем понимать область действия СОИБ. Под подконтрольным объектом будем понимать объект информационной инфраструктуры организации БС РФ, для которого применимы конкретные технологии и методы защиты (например, сервер, приложение или вычислительная сеть).

1. Моделирование как процесс ИБ

Как отмечено и в комплексе стандартов СТО БР ИББС, и в литературе [4], один из важнейших инструментов противодействия злоумышленнику — основанный на опыте прогноз. В сфере ИБ для прогнозирования, как правило, используются модели угроз и нарушителей ИБ. При разработке моделей используются имеющийся у организации опыт и знания, поэтому чем выше знания, тем точнее прогноз.

Рассмотрим подробнее процесс моделирования ИБ.

Вначале эксперт знакомится с объектом защиты, тем самым создавая (не всегда формально) модель объекта защиты. Далее он рассматривает возможные угрозы, применимые к данному объекту защиты, опираясь на специфику объекта защиты (в том числе уязвимости объекта защиты), выраженную в модели объекта защиты. В итоге эксперт получает модель угроз ИБ. Угрозы можно брать из каталогов угроз ИБ, но в то же время могут существовать угрозы, характерные только для определенного объекта защиты. Далее на основе модели угроз эксперт формирует модель нарушителя. На основе перечисленных трех моделей создается модель противодействия, некая стратегия противодействия угрозам ИБ (согласно модели угроз ИБ), реализуемым нарушителями ИБ (согласно модели нарушителя ИБ) в условиях данного объекта (согласно модели объекта защиты). Данная последовательность процедур моделирования изображена на рис. 1.

Рис. 1. Последовательность создания моделей ИБ

Модели могут быть как формализованными, так и неформализованными. Как правило, при создании СОИБ организации происходит высокоуровневое моделирование, создаются неформализованные модели, которые образуют следующий возможный комплекс документов:

1. Концепция обеспечения ИБ организации;
2. Политика ИБ организации;
3. Модель угроз;
4. Модель нарушителей.

При отладке процессов ИБ в организации могут создаваться частные политики и модели.

Модели могут быть как статические, так и динамические (то есть оценки могут меняться в зависимости от изменений в объекте защиты или в зависимости от данных мониторинга или аудита ИБ) [5].

2. Структура организации БС РФ и ее анализ с точки зрения разграничения доступа и мониторинга ИБ

Как уже было отмечено выше, до начала процесса моделирования угроз и нарушителей ИБ обязательно происходит процесс моделирования и описания структуры объекта защиты. Данный этап не всегда формализован, но он всегда присутствует.

В стандарте СТО БР ИББС-1.0-2010 [2] введена следующая структурированная модель объекта защиты:

1. Уровень физический (линии связи, аппаратные средства и пр.);
2. Уровень сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
3. Уровень сетевых приложений и сервисов;
4. Уровень операционных систем (ОС);
5. Уровень систем управления базами данных (СУБД);
6. Уровень банковских технологических процессов и приложений;
7. Уровень бизнес-процессов организации.

Следует отметить, что данная модель является моделью информационной инфраструктуры и не охватывает аспекты физической защиты.

Для охвата также уровня физической защиты целесообразно использовать семирубежную модель защиты информации (ЗИ) [6]:

1. Периметр контролируемой территории;
2. Здания, расположенные на территории;
3. Помещения внутри здания, в которых расположены ресурсы автоматизированной системы (АС) и защищаемая информация;

4. Ресурсы, используемые для обработки и хранения информации, и сама защищаемая информация;

5. Линии связи, проходящие в пределах одного и того же здания;

6. Линии (каналы) связи, проходящие между различными зданиями, расположенными на одной и той же охраняемой территории;

7. Линии (каналы) связи, проходящие по неконтролируемой территории.

Определим следующую структуру объекта защиты, подходящую для целей статьи (модель объекта защиты) (см. таблицу 1). Данная модель изображена на рис. 2.

Таблица 1. Структура организации БС РФ как объекта защиты

Название	Описание
Внешний контур	Средства внешней видеорегистрации, периметрическая защита, контроль доступа сотрудников или посетителей в здания организации — объекта защиты, также контроль за утечкой информации по побочным электромагнитным излучениям и наводкам, виброакустическому и прочим техническим каналам.
Помещение	Разграничение на уровне помещений: система контроля и управления доступом в помещения объекта защиты, видеорегистрация коридоров, датчики движения и т. п.
Внутри помещений	Регистрация и контроль действий субъекта доступа внутри помещения, в которое он получил доступ: система внутренней видеорегистрации, датчики движения (инфракрасные регистраторы), также контроль за использованием аппаратуры съема информации (например, фотоаппарат, устройство съема звуковой информации).
СЗИ от НСД	Контроль и разграничение доступа к объектам вычислительной техники внутренней сети организации: система защита информации от несанкционированного доступа.
Контроль ввода/вывода	Контроль за входящей/исходящей информацией: включает в себя контроль устройств ввода/вывода, проверку входящей информации на наличие вредоносного программного обеспечения, реализацию и контроль за реализацией отделения сегментов внутренней сети организации от сети, из которой имеется доступ к сети Интернет, а также средства разработки, на уровне не выше сетевого уровня эталонной модели взаимодействия открытых систем (OSI), а также контроль за информацией, поступающей по электронной почте. Сюда не входит контроль за информацией, поступающей по специальным защищенным каналам.
Операционные системы	Контроль и разграничение доступа субъекта на уровне операционной системы средства вычислительной техники, к которому он получил доступ.
ЛВС	Контроль и разграничение доступа субъекта доступа между объектами внутренней сети организации (уровень локальной вычислительной сети – ЛВС).
Приложения	Контроль и разграничение доступа на уровне приложений, в частности учетных операционных систем (УОС).
СУБД	Контроль и разграничение доступа на уровне баз данных.

Защищенные каналы	Контроль за информацией, поступающей по защищенным каналам, и контроль состояния самих каналов.
Антивирусная защита	Защита информации от воздействия вредоносного кода.
Непрерывность бизнеса	Обеспечение непрерывности бизнеса. Сюда входит обеспечение катастрофоустойчивости, анализ человеческих ресурсов и таких ресурсов, как здания и помещения.

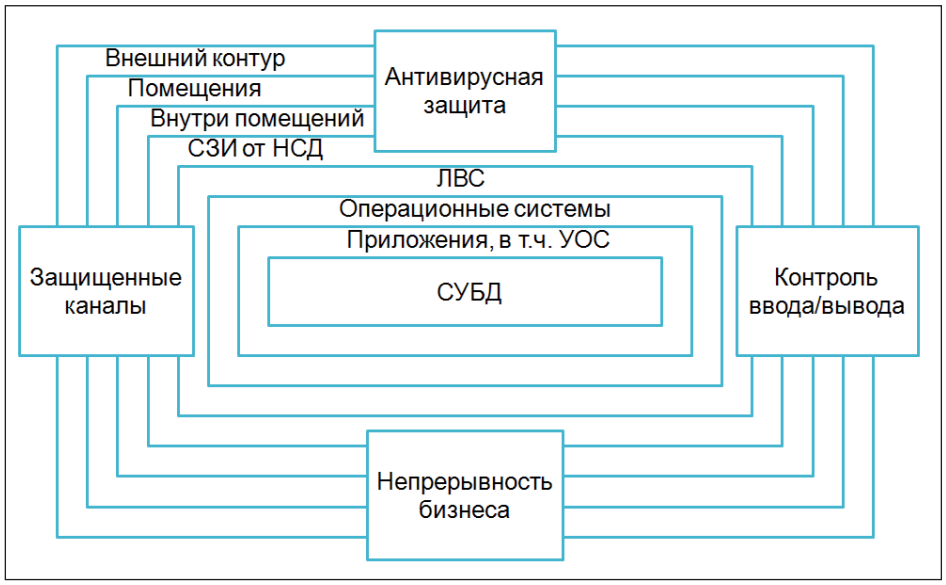

Рис. 2. Модель организации БС РФ как объекта защиты

Отметим также, что в данную классификацию не попал уровень бизнес-процессов организации. Защита на уровне бизнес-процессов заключается именно в разработке, внедрении, оценке и совершенствовании СОИБ с ориентацией на бизнес-цели конкретной организации [7].

Выделение специализированных уровней, таких как контроль за входящей/исходящей информацией и уровень антивирусной защиты, позволяет предполагать, что в критически важных сегментах сети организации БС РФ отсутствует вредоносное ПО и средства разработки ПО. Ввиду этого на уровнях СЗИ от НСД, операционных систем, ЛВС, прикладного ПО и СУБД можно применить единый подход по обеспечению ИБ: осуществить разграничение доступа для уменьшения возможности злоумышленных действий и осуществлять мониторинг ИБ. Причем для разграничения доступа и уменьшения возможностей привилегированных пользователей желательно применить эшелонированную (двойную) систему разграничения.

Целесообразно осуществлять мониторинг ИБ всех уровней (возможно, кроме уровня внешнего контура) из единого центра. Это позволяет оператору системы мониторинга получить полную картину происходящего в организации БС РФ.

3. Создание модели подконтрольного объекта и модели информационных технологий, реализованных на подконтрольном объекте

Для качественной настройки СОИБ необходимо понимать структуру подконтрольного объекта. Также необходимо понимать принципы функционирования ОС подконтрольного объекта:

- через какие интерфейсы можно осуществить интерактивный вход в ОС;
- какими способами можно реализовать запуск исполняемых объектов в ОС;

- каким образом реализуется разграничение доступа в данной ОС;
- в каком виде хранятся параметры защиты структур данных подконтрольного объекта;
- какие существуют основные подсистемы данной ОС;
- каким образом осуществляется ввод-вывод;
- какие существуют структуры данных в данной ОС;
- какие механизмы журналирования и управления реализованы в данной ОС;
- какие системные учетные записи (СУЗ) существуют в данной ОС и какими критичными системными ресурсами данная ОС обладает и т. д.

Далее необходимо четко определить, какое прикладное ПО установлено на подконтрольном объекте и какие реализуются информационные технологии. Необходимо понимать, какие технологические учетные записи (ТУЗ) существуют на подконтрольном объекте, какие действия в системе они производят. Данная информация должна содержаться в документации на АС.

4. Классификация информационных активов

Информационный актив, согласно [2], — информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации БС РФ; находящаяся в распоряжении организации БС РФ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

А классификация информационных активов, согласно тому же стандарту, — разделение существующих информационных активов организации БС РФ по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

Необходимо выделить основные критичные категории информационных активов, такие как:

1. Важная банковская информация (платежная, аналитическая). На уровне ОС данная информация, как правило, представляется либо в виде отдельных структур данных (файлов, наборов данных), либо в виде элементов баз данных, в конечном счете представляющих собой также некоторые структуры данных на дисковом пространстве;
2. Структуры данных, хранящие настройки средств ЗИ;
3. Структуры данных, содержащие информацию, необходимую для аутентификации, регистрации, идентификации и авторизации;
4. Структуры данных, содержащие правила разграничения доступа и другие настройки безопасности подконтрольного объекта;
5. Конфигурационные файлы СУБД, хранящей важную банковскую информацию;
6. Структуры данных, критичные для функционирования системы (системного ПО);
7. Структуры данных, критичные для функционирования прикладного ПО;
8. Иные информационные активы.

Также следует выделять отдельные информационные активы, необходимые для реализации информационных технологий подконтрольного объекта.

Под информационной технологией понимаем некую документированную последовательность действий на подконтрольном объекте, которая выполняется для достижения некоторой цели. К примеру, если специализированная учетная запись осуществляет подготовку данных для выгрузки в архивную систему, то данную учетную запись будем называть технологической (если с ее использованием невозможно выполнить интерактивный вход в ОС), а саму последовательность действий — информационной технологией, реализующей архивирование.

5. Классификация учетных записей. Ролевая структура и ее важность для организации БС РФ

Разделение должностных обязанностей, как правило, производится в виде ролей [8]. Роль — это зафиксированный набор некоторых документированных функций, должностных инструкций,

которые должен выполнять сотрудник, назначенный на данную роль. Сотрудник организации БС РФ может быть назначен сразу на несколько ролей. Причем совмещение некоторых ролей, согласно комплексу СТО БР ИББС, недопустимо.

Для построения четкой структуры разграничения доступа на подконтрольном объекте крайне желательно реализовать структуру с жесткой групповой привязкой.

Для выполнения каждой из существующих функций создается группа. Роль взаимно-однозначно идентифицируется набором групп. Для каждой роли каждого сотрудника организации БС РФ создается отдельная (персонифицированная) учетная запись. Эта структура обеспечивает прозрачность ролевой структуры на уровне мониторинга ИБ и дает возможность однозначно идентифицировать сотрудника и роль, которую он выполняет. Данная структура изображена на рис. 3.

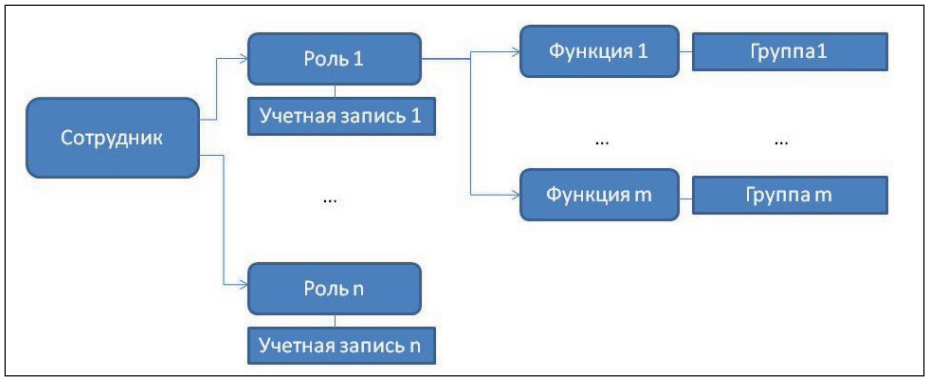

Рис. 3. Ролевая структура подконтрольного объекта с жесткой привязкой по группам

Данную структуру возможно реализовать на подконтрольных объектах, в которых управление полномочиями учетных записей осуществляется при помощи групп.

Введем определения особых учетных записей:

Системная учетная запись — учетная запись, необходимая для функционирования системного ПО.

Технологическая учетная запись — учетная запись, необходимая для функционирования прикладного ПО. Данная трактовка ТУЗ является упрощенной, под ТУЗ можно понимать учетную запись, от имени которой реализуется некоторая технология. Но для упрощения терминологии будем использовать первое определение.

Отметим также возможные методы деактивации учетной записи:

1. Учетная запись может быть деактивирована средствами ОС (технический метод);

2. Учетной записи может быть назначен пароль, удовлетворяющий требованиям парольной политики организации БС РФ, который далее разделяется между подразделениями организации БС РФ и находится под защитой (организационный метод).

Учетные записи, под которыми не планируется интерактивный вход в ОС, должны быть обязательно деактивированы. При наличии технической возможности запуска системных (технологических) задач с использованием данной учетной записи в деактивированном состоянии допускается деактивация техническим методом (относится к СУЗ и ТУЗ). При отсутствии данной возможности необходимо деактивировать учетную запись организационным методом. Возможно использование двух методов одновременно.

Отметим также, что существует два режима функционирования АС и подконтрольного объекта: штатный и нештатный. Штатный режим — режим функционирования АС, определенный документацией на АС.

Для проведения некоторых работ на подконтрольном объекте может потребоваться учетная запись с критично большим для ИБ подконтрольного объекта набором полномочий. Данная

учетная запись считается учетной записью нештатного режима функционирования (НШР). Ее использование допускается только в нештатном режиме функционирования АС при наличии письменного разрешения. В штатном режиме работы данная учетная запись должна быть деактивирована техническим и организационным методом.

Приведем базовую классификацию учетных записей подконтрольного объекта:

1. СУЗ;
2. ТУЗ;
3. Учетные записи НШР;
4. Учетные записи, имеющие привязку к конкретному сотруднику организации БС РФ.

Отметим, что назначение сотрудника на роль должно определяться приказом организации, в этом же приказе должна быть указана привязка роли к учетной записи сотрудника. Также необходим документ, в котором зафиксировано соответствие функций и групп ОС (при официальном принятии данной жесткой ролевой структуры в организации БС РФ).

Заключение

В статье рассмотрены процессы моделирования, классификации информационных активов и учетных записей, их место и роль в организации БС РФ. Предложена модель организации БС РФ как объекта защиты, модель конкретного подконтрольного объекта на объекте защиты. Также выделены основные типы информационных активов и учетных записей в организации БС РФ.

Внедрение и улучшение процессов моделирования, классификации информационных активов и учетных записей в организации БС РФ позволяет осуществить эффективные мониторинг ИБ и защиту информации от несанкционированного доступа, а также совершенствовать СОИБ организации в целом.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г.
2. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2010).
3. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008.
4. *Курило А. П. [и др.]*. Обеспечение информационной безопасности бизнеса. М: БДЦ-пресс, 2005.
5. *Атаманов А. Н.* Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах. Дисс. … канд. тех. наук. М.: НИЯУ МИФИ, 2012.
6. *Герасименко В. А., Малюк А. А.* Основы защиты информации. М.: МИФИ, 1997.
7. *Малюк А. А.* Теория защиты информации. М.: Горячая линия – Телеком, 2012.
8. *Выборнов А. О., Курило А. П., Харламов В. П.* Ролевая модель сотрудников банковской организации в области информационной безопасности // Безопасность информационных технологий. 2012. № 3. С. 90–96.