УДК 81.93.29

Крыжевич Леонид Святославович, канд. тех. наук,
и.о. заведующего кафедрой информационной безопасности
Курский государственный университет

Швецова Мария Валерьевна,
Бакалавр третьего года обучения по направлению подготовки
Информационная безопасность (профиль Безопасность компьютерных систем
(в сфере техники и технологии)), Курский государственный университет

ПОСТРОЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ФИНАНСОВОЙ ОРГАНИЗАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Аннотация. В статье рассматривается защита информации от несанкционированного доступа, характеризуется информационная инфраструктура АО «Альфа-Банк» и анализируется используемые автоматизированные системы на предмет угроз и рисков кибербезопасности. Представлены требования к комплексной системе защиты информации банка в современных условиях развития информационных технологий.

Abstract. The article examines the protection of information from unauthorized access, characterizes the information infrastructure of Alfa-Bank JSC and analyzes the automated systems used for threats and risks of cybersecurity. The requirements for the bank's integrated information security system in modern conditions of information technology development are presented.

Ключевые слова: несанкционированный доступ, информация, угроза, риск, защита, безопасность.

Keywords: unauthorized access, information, threat, risk, protection, security.

Частота несанкционированного доступа к информации в информационных системах (ИС) в процессе их интеграции и использования неуклонно растет, что неизбежно приводит к огромным финансовым и материальным потерям. Исходя из этого возникает большое количество рисков и угроз в области обеспечения безопасности информационной среды. Поэтому проблема защиты информации, в частности, экономической, стоит остро, и является на сегодняшний день крайне актуальной.

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации. Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности, ведущую за собой ущерб [3].

Проявления возможного ущерба могут быть различны:

– моральный и материальный ущерб деловой репутации организации;

– моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

– материальный ущерб от разглашения защищаемой (конфиденциальной) информации и др.

Носителями угроз безопасности информации являются разные источники. Их можно разделить на три основные группы:

1) антропогенные источники угроз;

2) техногенные источники угроз;

3) стихийные источники угроз.

Угрозы как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости. Уязвимости безопасности информации могут быть:

1) объективными;
2) субъективными;
3) случайными.

В условиях сегодняшней цифровизации экономических отношений, экономическая безопасность в системе национальной безопасности играет фундаментальную роль. Основной элемент обеспечения экономической безопасности коммерческого банка – это его финансовая, информационная, инвестиционная и инновационная защищенность от возможных угроз.

К объектам несанкционированного доступа банка можно отнести следующие элементы:

– капитал банка;
– ведение текущей деятельности банка;
– деловая репутация;
– порядок функционирования и управления деятельностью банка;
– физические и радиоэлектронные.

Согласно статистике Банка России, в 2022 году объем операций без согласия клиентов увеличился по сравнению с 2021 годом на 4,29% на фоне активного развития новых дистанционных платежных сервисов и роста объема денежных переводов с применением электронных средств платежа [7].

Для снижения кредитных и информационных рисков банкам необходимо иметь эффективное подразделение, способное быстро реагировать на угрозы защиты информации от несанкционированного доступа и применять своевременные меры по их предупреждению и снижению негативных последствий.

Согласно Государственному стандарту РФ ГОСТ Р 50922–2006, защита информации от несанкционированного воздействия (ЗИ от НСВ) – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации [1].

Согласно Приказу ФСТЭК России от 18.02.2013 N 21, в состав мер по обеспечению безопасности данных входят:

– идентификация и аутентификация субъектов доступа и объектов доступа;
– защита технических средств;
– защита информационной системы, ее средств, систем связи и передачи данных;
– управление конфигурацией информационной системы и др. [2].

В основу систем защиты информации также входят принципы защиты информации от несанкционированного доступа, такие как: принцип обоснованности доступа, принцип достаточной глубины контроля доступа, принцип разграничения потоков информации, принцип чистоты повторно используемых ресурсов, принцип персональной ответственности и принцип целостности средств защиты.

Основываясь на данных принципах, можно выделить основные средства и способы защиты информации. К средствам относятся физические, аппаратные, организационные и программные. Способами защиты информации выступают препятствие, регламентация, управление, побуждение и принуждение.

В свою очередь, для обеспечения защиты информации от несанкционированного доступа используют комплекс методов, среди которых технические, физические, математические и др. К базовым техническим методам ЗИ от НСД относят:

– шифрование данных (крипто-стеганография);
– защита важной информации и предотвращение утечек («Data Loss Prevention» – «Information Rights Management»);
– управление неструктурированными данными («Data Governance»)
– контроль печати.

К физическим методам относят:

– механические преграды;
– датчики;
– средства идентификации личности;
– устройства зашумления/помехоподавляющие фильтры и др. [4].

Рассмотрев теоретические аспекты информационной безопасности, перейдем к структуре информационной системы АО «Альфа-Банк» и проанализируем ее на предмет угроз и рисков безопасности.

Компонентами системы являются технические средства, обеспечивающие обработку и хранение информации Централизованной базы данных и Распределенного реестра. Компонентами информационной системы банка являются:

– личный кабинет физического лица (ЛКФЛ), личный кабинет юридического лица (ЛКЮЛ);
– ядровые сервисы;
– оператор (банк);
– ноды системы;
– модуль смарт-контрактов.

Работа системы обеспечивается алгоритмами. Их корректность в системе достигается за счет:

– отсутствия возможности внесения изменений в установленные оператором алгоритмы иными лицами;
– применения на каждой ноде системы криптографии, шифрования и защиты каналов для передачи данных, и др.

Основной целью оператора (банка), является защита пользователя от возможного нанесения ему материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию. Минимизация уровня операционного и других рисков оператора, достигается посредством: доступности, целостности и конфиденциальности информации. Оператор обеспечивает защиту информации, получаемую, подготавливаемую, обрабатываемую, передаваемую и хранимую в системе, с соблюдением мер безопасности, описанных в Законодательстве РФ и в своде правил информационной системы «Альфа-Банк» [6].

К некоторым из них относятся:

– многофакторная аутентификация пользователя при осуществлении доступа в систему;
– контроль и определение лиц, совершающих сделки;
– использование специализированных программных средств для хранения технологических ключей нод системы;
– защита от вмешательства в процесс функционирования системы посторонних лиц;
– защита от несанкционированной модификации и контроль целостности используемых в системе программных средств, и др.

Как показывает статистика, ежеквартально увеличивается число кибератак в промышленных крупных компаниях, госсекторе, IT–компаниях, однако в финансовом секторе, в частности, в коммерческих банках, наблюдается спад таких атак благодаря правильно выстроенной системе шифрования данных. Особенно это заметно в сфере электронного банкинга.

Например, в «Альфа-Клиент Онлайн» – банкинг-приложении от «Альфа-Банка» используется система криптозащиты: стойкий криптоалгоритм на основе битного ключа, который шифрует персональные данные клиентов. Но насколько бы не выступала безопасной среда электронного банкинга, в данном случае, мобильного, главная угроза кибербезопасности заключается в самом клиенте и его устройстве. Рассматривая финансовый фишинг и банковские вредоносные программы как часть кибератак, рекордный пиковый уровень финансовых фишинговых атак был достигнут в 2017г. (53,8%) [5].

Среди банковских вредоносных программ в 2022г. наиболее динамичными по уровню распространения среди финансовых киберпреступников стали такие банковские вредоносные программы как «Zbot», «SpyEye», «CliptoShuffler», «Emotet», лидирующее место из которых занимает «Zbot», с помощью которой была совершена приблизительно пятая часть (21,6%) кибератак.

В ходе проведенного исследования было выявлено, что одними из основных причин появления угроз и рисков кибербезопасности в условиях применения системы электронного банкинга являются:

– уязвимости аппаратно-программного обеспечения (в т.ч. систем электронного документооборота (СЭД));

– отсутствие должной достоверности контроля выполнения технических требований;

– неосведомленность и низкая ответственность персонала.

В АО «Альфа-Банк» в настоящее время внедрена российская система электронного документооборота «WSS Docs». В данной системе автоматизированы процессы делопроизводства в области создания и регистрирования документов, контроля маршрута согласования, подписания, утверждения, а также хранения документов. Общий риск использования СЭД состоит в особенности самой системы, так как вся информация и документация консолидируется в одном месте. К возможным типовым и частым угрозам безопасности для системы электронного документооборота мы отнесем:

– целостность информации;

– нарушение конфиденциальности;

– нарушение нормального функционирования системы.

К защите и безопасности электронного документооборота как одному из аспектов информационной среды банка, необходим комплексный подход.

По нашему мнению, необходимо защищать, во-первых, аппаратные элементы системы (учитывая, что рассмотренная WSS Docs, как и большинство СЭД – консолидирована в одном месте). Во–вторых, важно уделить особое внимание защите файлов системы. Это файлы программного обеспечения и базы данных. В–третьих, необходимо защищать документы и информацию, находящиеся внутри системы.

АО «Альфа-Банк» с 2011 года состоит в партнерстве с «Лабораторией Касперского» и применяет несколько передовых защитных решений, которые в совокупности позволили обезопасить большинство наиболее уязвимых для атак секторов инфраструктуры. Этими решениями выступают «Kaspersky Embedded Systems Security» и «Kaspersky Endpoint Security» для бизнеса.

Также банк использует платформу от SecurityVision «SOAR» – платформу, обеспечивающую сбор данных о событиях, инцидентах информационной безопасности из нескольких источников, координацию (оркестрацию) и автоматизацию реагирования на выявленные инциденты информационной безопасности [8].

Напрашивается вывод, что технические средства защиты информации в банке, несомненно, являются эффективными. Но помимо того, что компьютерная безопасность в рассматриваемом банке находится на должном уровне, следует выделить несколько иных направлений в совершенствовании механизма обеспечения информационной безопасности в коммерческом банке.

Безопасность коммерческого банка представляет собой защищенное положение собственника кредитной организации, управляющих и клиентов банка, также безопасность информации и материальных ценностей от различных факторов. Построение системы обеспечения безопасности информации банка, и ее функционирование должны осуществляться в соответствии со следующими основными принципами: законность, экономическая целесообразность, сочетание превентивных и реактивных мер, обоснованность, комплексность и непрерывность.

Для минимизации выявленных угроз и рисков требуется комплексная система защиты:

– защита аппаратных и программных элементов системы (учитывая, что рассмотренная WSS Docs, как и большинство СЭД – консолидирована в одном месте);

– подбор квалифицированных аудиторов и консультантов в области информационной безопасности;

– углубленная подготовка персонала, в особенности ИБ/ИТ–администраторов.

Наличие нормативно–правовой базы позволяет выстроить определенные регламенты функционирования автоматизированных банковских систем. Мы рассмотрели сертифицированные средства защиты информации от несанкционированного доступа для комплексного предотвращения обнаруженных возможных угроз и остановили выбор на «Secret Net Studio». Данный продукт обладает всеми возможностями в плане контроля целостности системы для минимизации угроз и рисков несанкционированного доступа к информации, а именно:

– возможностью работы со смарт–картами JaCarta;

– поддержкой контроля реестра;

– возможностью контроля неизменности аппаратной конфигурации компьютера, блокировки компьютера при подключении или отключении заданных устройств;

– поддержкой теневого копирования информации, выводимой на внешние носители.

При правильном использовании средств программного обеспечения, Secret Net Studio позволяет разграничить доступ к защищаемым ресурсам организации, в т.ч. облачным, а также обеспечить контроль целостности к защищаемым ресурсам объектов информатизации, регистрации и учета фактов несанкционированного доступа к защищаемым ресурсам и главное – к СЭД.

Также Secret Net Studio обладает следующими защитными механизмами СЗИ от НСД:

– механизм защиты входа в систему;

– механизм разграничения доступа и защиты ресурсов;

– механизм контроля и регистрации.

Таким образом, в результате анализа автоматизированных систем, угроз безопасности информации и информационных рисков АО «Альфа-Банка», можно подчеркнуть, что комплексная система защиты должна всегда совершенствоваться с учетом появления новых операций, функций, а также, что в организации необходимо трезво оценивать возможные угрозы и риски защиты аппаратных средств системы, персональных компьютеров, в частности, СЭД, и величину возможных потерь от реализованных угроз.

Список литературы:

1. «ГОСТ Р 50922–2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373–ст)

2. Приказ ФСТЭК РФ от 05.02.2010 N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (Зарегистрировано в Минюсте РФ 19.02.2010 N 16456)

3. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. //. Классификация угроз информационной безопасности // Символ науки. 2016. №9–1. – С. 145–147

4. Зайцева А.П. Технические средства и методы защиты информации: Учебник для вузов / Под ред. А. П. Зайцева, Р. В. Мещерякова, А. А. Шелупанова. М.: "Горячая линия–Телеком". – 2018. – 442

5. Султыгова, А.А., Кунцман, М.В. Киберпреступность как следствие цифровизации экономики [Текст] / А.А. Султыгова, М.В. Кунцман // Economy and Business. – 2021. – № 9–2 (79). – С. 88–91

6. Правила информационной системы АО «АЛЬФА–БАНК» – [Электронный ресурс]: URL: https://alfabank.servicecdn.ru/site–upload/cc/9d/4739/Pril_Pravila_informacionnoi_sistemy_AO_ALFA–BANK.pdf

7. Обзор операций, совершенных без согласия клиентов финансовых организаций [Электронный ресурс]: – URL: https://www.cbr.ru/analytics/ib/operations_survey_2022
8. Security Vision Security Orchestration, Automation and Response (SOAR) – [Электронный ресурс]: URL: https://www.securityvision.ru/products/soar/