СПЕЦИФИКА ПРОЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВОМ СЕКТОРЕ

Вишнякова Алена Владимировна

студент 3 курса, Институт экономики и предпринимательства Нижегородский Государственный Университет им. Н. И. Лобачевского, РФ, Нижний Новгород

Финансовый бизнес в России относится к наиболее зрелым в области информационной безопасности. Вместе с тем радикальные изменения в сфере ИТ, связанные с масштабной виртуализацией ИТ-ресурсов, с распространением мобильного доступа, с переходом к облачной ИТ-инфраструктуре как на стороне самих финансовых организаций, так и на стороне их клиентов, заставляют участников финансового бизнеса, охватывающего практически все государственные и частные структуры наряду с частными лицами, использовать новые технологии и средства обеспечения информационной безопасности.

Как отмечают Дорожкин А.В. и Ясенев В.Н. под обеспечением информационной безопасности предприятия подразумевается взаимосвязанное решение двуединой задачи: с одной стороны, защита информации от ее разрушения и несанкционированного обращения с нею, с другой - защита людей и информационно-управляющих систем от разрушающего воздействия информации [3, с. 812].

Операционная деятельность финансовых структур, связанная непосредственно с деньгами, особенно привлекательна для киберзлоумышленников. Специалисты в области информационной безопасности по-прежнему видят большие проблемы в защищенности дистанционного банковского обслуживания (ДБО). Мошенничество в банковской сфере, наносящее значительный ущерб, заставляет банки внедрять дорогие системы борьбы с преступниками [1].

С ростом новых систем и направлений в секторе растёт и в безопасных технологиях и защиты своего Обнаружение в какой-отрасли рисков безопасности является причиной появления проектов, требующих исследований, проверок.

Всё, связано непосредственно с деньгами, всегда наиболее притягательным преступников. Но если финансовые организации центры аккумулирования и потоков денежных были сосредоточены в на вопросах физической материальных ценностей, то в эпоху перевода активов и платежей в форму с широким информационно-телекоммуникационных намного актуальнее банков стали безопасности информационной.

Проекты, связанные с информационной безопасностью всегда требуют доскональной проработки от создания нового подразделения и набора людей до выстраивания операционного взаимодействия между подразделениями-участниками. Это необходимо для обеспечения сохранности информации в целом и для сохранения денежных средств, если рассматривать финансовый сектор отдельно. Различных способов киберпреступности и мошенничества в сфере высоких технологий становится все больше с каждым разом.

В финансовом секторе риски информационной безопасности всегда являются самыми высокими. Поэтому разрабатывается, большое количество мер и способов, по снижению или устранению их. Стоит отметить, что и оценка рисков сыграет немаловажную роль в этом деле, так как если риски компании будут не существенными, то нет смысла затрачивать большие денежные средства на хоть и качественную, но дорогостоящую защиту информационной безопасности.

Вишнякова А.В. Специфика проектов информационной безопасности в финансовом секторе // Молодежный научный форум: Общественные и экономические науки: электр. сб. ст. по мат. XL междунар. студ. науч.-практ. конф. № 11(40). URL: https://nauchforum.ru/archive/MNF_social/11(40).pdf (дата обращения: 27.08.2025)

Для снижения рисков информационной безопасности необходима не только определенная программа, помогающая снизить риски, а целые комплексы или наборы программ, решающие многие проблемы информационной безопасности.

При разработке проекта по информационной безопасности, во-первых, следует изучить какие угрозы (внешние или внутренние) стоят перед компанией, откуда они появились, и каким образом могут повлиять на инфраструктуру финансовой организации. Затем следует разрабатывать методики противодействия и оценку их целесообразности. Базовыми и основными процессами и технологиями являются: управление уязвимости, наличие систем обнаружения и предотвращения вторжений, а также защиты от мошенничества. Как дополнительные могут использоваться посторенние процессов сбора и корреляции событий, проверка кода на его качество и безопасность [2].

Поскольку финансовые организации действуют в условиях сильной конкуренции, они стараются оперативно выводить на рынок новые банковские продукты, для чего весьма подходит онлайновая среда, интернет-банкинг. А это порождает новые для банковского бизнеса ИБ-риски и, как следствие, вызывает необходимость разрабатывать и использовать новые ИБ-средства.

Однако, несмотря на высокую конкуренцию, банки ведут относительно консервативную политику в области внедрения новых ИБ-технологий. На наш взгляд, такую стратегию можно назвать правильной в нынешних условиях, когда доходы у банков не так велики, как хотелось бы.

Вместе с тем в технологическом консерватизме в области информационной безопасности есть и отрицательные моменты: поскольку участники рынка ДБО не спешат менять используемые средства защиты на более стойкие, технологии и инфраструктура, используемые сегодня в банках, не всегда способны защитить ДБО от высокотехнологичных атак.

Конечно же, для определенной компании не обязательно наличие всех этих видов защиты, набор таких технологий может отличаться. При этом следует помнить, что работать эффективно эти процессы будут при наличии в организации основного уровня защиты. Таким уровнем являются: антивирусная защита, парольная политика, защита Интернет и почтовых шлюзов и другие.

Как показывает практика, что в 95% случаев мошенничества происходит по вине клиентов [2]. Однако любая компания должна обеспечивать безопасность транзакций, защиту прав и свобод человека и гражданина при обработке его персональных данных, при всем этом и сохраняя свою репутацию и позиции среди других фирм. Другими словами, компания должна осуществлять проекты, направленные на предотвращение утечек конфиденциальной информации (выполнение обязательств в связи с 152-ФЗ «О персональных данных») [4]. Внедрение приложения по обеспечению безопасности для финансовых групп, мобильные банкинги, SMS-подтверждения о совершившихся транзакциях и операциях: все это примеры мер по защите информационной безопасности в финансовой отрасли.

Таким образом, появление и реализация различных проектов по защите информационной безопасности в финансовом секторе не обеспечит абсолютной безопасности. Необходимо обновлять имеющиеся проекты и внедрять новые разработки технологий защиты информации, как только появились новые угрозы или риски.

Список литературы:

1. Васильев В. Информационная безопасность в финансовом секторе – [Электронный ресурс]. – Режим доступа: https://www.pcweek.ru/security/article/detail.php?ID=156455.

2. Воронова М. Специфика проектов информационной безопасности в финансовом секторе – [Электронный ресурс] – Режим доступа: http://www.itsec.ru/articles2/person/spetsifika-proektov-informatsionnoy-bezopasnosti-v-finansovom-sektore .

3. Дорожкин А.В., Ясенев В.Н. Информационная безопасность как инструмент обеспечения экономической безопасности хозяйствующего субъекта // Экономика и предпринимательство, № 5 (ч.1), 2015 г. С. 812–816.

4. Федеральный Закон «О персональных данных» от 27.07.2006 № 152-ФЗ.