УДК 004.056.53

Кирсанов И.Р., Студент
МГТУ им. Н.Э. Баумана
Россия, г. Москва
Полухина Д.Ю., Студент
МГТУ им. Н.Э. Баумана
Россия, г. Москва

МЕХАНИЗМ РЕАЛИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ, ЗАНИМАЮЩИХСЯ ФИНАНСОВОЙ ДЕЯТЕЛЬНОСТЬЮ.

Аннотация: *Статья отражает основные проблемы информационной безопасности финансовых предприятий. Рассмотрены основные угрозы информационной составляющей, предложены методики предотвращения информационных инцидентов. Рассмотрен вопрос запуска Security Operation Center для предприятия.*

Ключевые слова*: информационная безопасность, инцидент, информационная угроза, Security Operation Center.*

Kirsanov I.R., Student
BMSTU
Russia, Moscow
Polukhina D.Yu., Student
BMSTU
Russia, Moscow

The mechanism for implementing the security protection of enterprises engaged in financial activities.

Abstract: *The article reflects the main problems of information security of financial enterprises. The main threats to the information component are considered, methods of preventing information incidents are proposed. The issue of launching the Security Operation Center for the enterprise was considered.*

Keywords: *information security, incident, information threat, Security Operation Center*

Понятие «информационная безопасность» можно встретить на любом предприятии и производстве. Однако информационная защищенность предприятий, которые осуществляют финансовую деятельность, имеет ряд особенностей, обусловленных различными угрозами «публичности» (например, создание мобильных приложений для удобства пользования услугами). Вся конфиденциальная информация может оказаться в руках злоумышленников, при некачественной организации безопасности и защищённости таких данных.

Стратегия финансового предприятия в сфере противодействия угрозам безопасности информационной среды заключается в сбалансированном осуществлении взаимодополняющих мер, связанных с обеспечением безопасности: от организационных мер на высшем уровне управления до специализированных мер безопасности информации по каждому выявленному риску.

При создании системы информационной безопасности необходимо учесть функциональные требования:

- Обучение персонала и должностных лиц возможностям пользования полным спектром средств программного обеспечения в принятии ими решений;
- Соответствие условий хранения и шифрования информации исходя из её свойств и программных особенностей;
- Получение только той информации должностным лицом, соответствующей им замещаемой должности.

Для того, чтобы обеспечить безопасность на должном уровне в организационной структуре предприятия необходимо выделить специальный отдел или подразделение. К задачам ответственного

подразделения в соответствии с политикой информационной безопасности относят:

- определение потребностей в реализации мер по обеспечению информационной безопасности;
- соблюдение действующего законодательства, по обеспечению информационной безопасности, приватности и неразглашению;
- проверка, анализ и пересмотр внутренних нормативных документов с целью установления их соответствия политике обеспечения информационной безопасности.
- обучение и последующий контроль персонала в области обеспечения безопасности информации;
- выявление инцидентов информационной безопасности и оперативное реагирование на них;
- информирование руководства об угрозах и рисковых событиях информационной безопасности;
- прогнозирование и предупреждение инцидентов безопасности информации
- мониторинг и последующая оценка системы информационной безопасности предприятия и другие.

Изучение видов угроз и посягательств на безопасность является обязательной частью разработки мер по организации защиты информации. Это связано с тем, что четкое понимание характера и вида угроз позволяет формировать эффективную систему мер их выявления, предупреждения и последующего расследования.

Угроза в сфере информационной безопасности [3. с.156] есть потенциальная опасность завладения конфиденциальной информацией злоумышленниками. Рассмотрим основные угрозы информационной безопасности финансового предприятия. (Рис. 1)

Рис. 1 - Структура угроз информационной безопасности предприятия в 2002 и 2020 годах.

Основным направлением в системе обеспечения информационной безопасности является выбор персонала, его обучение и повышение квалификации. Разумно в контрактах, заключаемых между финансовым предприятием и сотрудниками четко оговаривать требования, ответственность за их нарушение, так как на практике, именно нарушение требований со стороны сотрудника приводит к утечке информации.

Помимо всего вышеперечисленного на каждую должность составляется профессиограмма - перечень личных качеств на данную должность включает, на которые основываются при подборе персонала.

Для наглядности реализации механизма по защите информации, рассмотрим требования и навыки к соискателю на должность «Начальник отдела информационной безопасности» одной и финансовых организаций.

Должностные обязанности:

1. Руководить отделом информационной безопасности;
2. Контролировать соблюдение политики конфиденциальности информационных потоков;
3. Организация обучения и переобучения, как нового персонала, так и действующих сотрудников;
4. Уметь работать с криптографическими ключами при сотрудничестве с органами, наделёнными властными полномочиями;
5. Проводить в случае необходимости служебного расследования;
6. Работать над ошибками в организации информационной безопасности;
7. Содействовать с сотрудниками первичного аудита;
8. Контролировать и координировать деятельность сторонних подразделений, которые имею доступ к конфиденциальной информации;

Требования к уровню подготовки кандидата:

1. Высшее образование по специальности «Информационная безопасность»;
2. Опыт работы на аналогичной специальности не менее трёх лет;
3. Навык анализа профессиональной литературы на английском языке;
4. Опыт создания и реализации проектов на предприятии;

Следующей мерой по обеспечению информационной безопасности можно считать зафиксированные положения и функции каждого подразделения, согласно которым составляются схемы, диаграммы, чертежи, на которых указано как должно выглядеть рабочее место исполнителя, его обязанности, уровень доступа к конфиденциальной информации.

Благодаря всем мерам, переведённым выше, можно сделать вывод, что такое разграничение позволяет каждому сотруднику четко понимать, что от него требуется, каким образом организована работа, кто отвечает за ту или иную информацию. Все это сводит к минимуму утечку информации со стороны сотрудников, и предотвращает внешние нападения со стороны конкурентов и мошенников.

Помимо «кадровых» рекомендаций по обеспечению информационной безопасности также стоит отметить и техническую сторону зашиты информации от утечек и несанкционированного доступа.

Одной из эффективных разработок в системе обеспечения информационной безопасности стал презентованный в мае 2016 года операционный центр информационной безопасности (SOC - security operation center), который основан на безе компании ArcSight ESM [2. с.258] - лидера в сфере решений по контролю случаев нарушения безопасности и уровня исполнения норм отраслевого регулирования.

Говоря про SOC, в первую очередь подразумевают новые технологии и методы управления, позволяющие значительно повышать результативность противодействия угрозам информационной безопасности как сегодня, так и в будущем. SOC — это не столько программное обеспечение или софт, сколько процессы управления рисками, моделирования угроз и их последующей оперативной обработки. Подобный технологический менеджмент в области информационной безопасности позволит предприятию защитить все то, что представляет для него наибольшую информационную ценность: активы и бизнес-процессы, деньги клиентов и свою собственную деловую репутацию.

Security operation center призван помогать решать основополагающие в информационной безопасности задачи:

1. Предоставлять отчеты аудиторским компаниям для выверки соответствия законодательным требованиям и стандартам;

2. Собирать и хранить файлы в едином пространстве;
3. Выполнять корреляционный и регрессионный анализ между событиями.

Основными функциями согласно классификации MITRE можно выделить (рис. 2):

Рис. 2-Классфикация функций SOC.

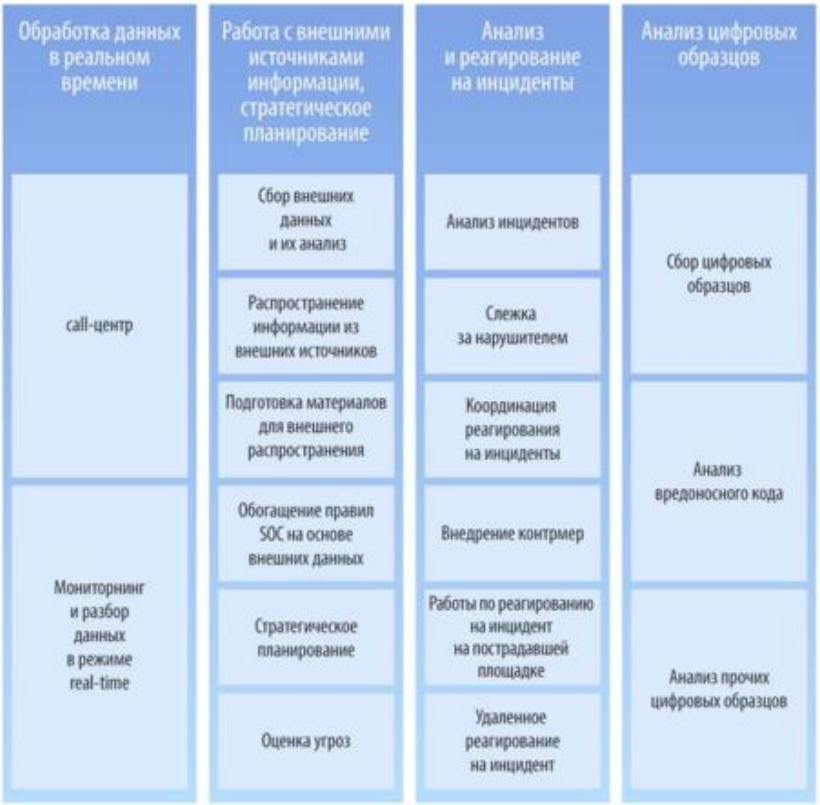

Рис. 3 -Классификация функций SOC.

Исходя из функций данного подразделения, стоит сделать вывод о том, что введение в организационную структуру такого подразделения. Позвонил осуществлять всесторонний мониторинг деятельности финансовой организации.

Подводя общую черту, стоит отметить, что за последние годы, в системе организации информационной безопасности произошли значительные изменения. Приняты и внедрены законы и нормативные акты, регулирующие данную сферу; найдены новые инструменты против внутренних и внешних угроз; обозначены перспективы и задачи развития в данном направлении. Рассмотрев, каким образом, организуется безопасность на финансовых предприятиях, можно сделать вывод о том, что Россия находится на достаточно высоком уровне знаний и умений в области защиты информации, и может развивать это в дальнейшем. Безопасность и защищенность информации является ключевым моментом, т.к. любой сбой или утечка информации несут резко отрицательные последствия и приводят к молниеносному развитию системного кризиса.

Меры по реализации эффективной системы безопасности рассмотрены не только со стороны кадрового обеспечения, мониторинга, но и со стороны IT. Для любого передового предприятия (не только финансового), внедрение отдела SOC позволит предотвратить утечку данных, которые могут нанести не только финансовый вред предприятию, но деловой репутации организации.

Список источников:

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.07.2016) «Об информации, информационных технологиях и о защите информации»
2. Арефкина Е.И Правовые основы информационной безопасности: учебник / Е.И Арефкина ,- М.: Проспект, 2018.- 367 с.
3. Перов С.И. Основные киберугрозы / С.И. Перов. - М.: Ярославль: Нюанс, 2017.-365 с.
4. Ханнанова Е.Н. Информационная безопасность. // [Электронный ресурс]. – Режим доступа: http://www.scienceforum.ru/2015/1005/9978