РАЗРАБОТКА АЛГОРИТМА ОБУЧЕНИЯ СОТРУДНИКОВ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Батожок И.А., студент гр. ИБ17-1, 4 курс
Научный руководитель: Хлудова О.Е., преподаватель
Государственное профессиональное образовательное учреждение Кузбасский колледж архитектуры, строительства и цифровых технологий
г. Новокузнецк

Обеспечение собственной информационной безопасности на предприятиях является частью общей системы управления, необходимой для достижения стратегических целей развития организации и создания основного продукта, а также для вспомогательных элементов деятельности, таких как коммерческие переговоры, ценовая политика и другое. В некоторых областях информационные системы обрабатывают сведения, составляющие не только коммерческую, но и государственную тайну, а также другие виды конфиденциальной информации.

Проблема защиты корпоративной информации существовала всегда. На сегодняшний день главными угрозами являются:

- фишинг и социальная инженерия;
- кликджекинг;
- программы-вымогатели;
- бесфайловые атаки;
- ботнеты;
- атаки типа man-in-the-middle.

Приведенные угрозы могут быть реализованы вследствие наличия следующих факторов:

- небрежности сотрудников;
- недостатка квалифицированных кадров;
- несогласованности и сложности систем внутри организации;
- действий злоумышленников-инсайдеров.

Реализация угроз безопасности может привести к:

- утечке персональных данных сотрудников и клиентов;
- несанкционированному доступу к финансовой информации организации;
- к порче репутации и потере клиентов.

За время пандемии проблема защиты корпоративной информации обострилась еще сильнее, в связи с переходом на удаленный режим работы.

По результатам исследования 2021 Data Privacy Benchmark Study, в отношении числа удаленных сотрудников российские организации распределились следующим образом:

- в 24% компаний доля удаленных сотрудников составляет 76-100%;

– в 31% предприятий 51-75% специалистов работают из дома;

– в 27% организаций удаленный формат взаимодействия используют 26-50% работников;

– в 18% компаний от 1 до 25% сотрудников выполняют свои обязанности в удаленном режиме [1].

Из-за перехода на дистанционный режим работы и учебы вскрылась проблема, связанная с контролем применения информации на смартфонах и домашних компьютерах сотрудников и обучающихся. Нехватка средств удаленной защиты информации и неэффективное применение VPN привело к тому, что корпоративные данные оказались под угрозой несанкционированного доступа. Таким образом, большое количество угроз может быть реализовано из-за невнимательности или незнания сотрудниками основ информационной безопасности. Значимость наличия знаний в области информационной безопасности становится тем более высокой, чем выше степень автоматизации бизнес-процессов предприятия и чем больше интеллектуальная составляющая его конечного продукта.

Департамент информационной безопасности является основной структурной единицей, которая отвечает за комплексную защиту информации на предприятии. Данное структурное подразделение выполняет работу с персоналом, направленную на защиту информационных активов в части подбора, расстановки и обучения сотрудников, связанных с обработкой информации. В задачи департамента входит:

– привлечение сторонних специалистов и исследователей для разработки политики безопасности;

– управление обучением персонала компании (обеспечение своевременности прохождения обучения и т.п.).

Инструктирование сотрудников основам информационной безопасности является только небольшой частью функциональных задач, возложенных на департамент. Организация процесса обучения сотрудников является трудоемкой задачей, если количество пользователей исчисляется сотнями и тысячами, а количество инцидентов в условиях перехода на удаленный режим работы растет. Таким образом, формирование гибкой системы обучения персонала информационной безопасности является актуальной задачей.

Целью данной работы является разработка подхода к обучению пользователей в области информационной безопасности, который позволит сотрудникам адекватно реагировать на инциденты.

Для достижения поставленной цели необходимо решить следующие задачи:

– проанализировать существующие корпоративные алгоритмы обучения сотрудников;

– сформировать предполагаемые сценарии обучения;

– разработать курсы и темы обучения.

На сегодняшний день во многих организациях недооценивается значение человеческого фактора в вопросах цифровой безопасности. Даже в случаях,

когда обучение персонала информационной безопасности признается руководством необходимым, выбираются неэффективные методы, которые зачастую носят формальный характер. Во многих компаниях с иностранными владельцами уже давно проводятся тренинги по повышению осведомленности персонала к атакам с использованием социальной инженерии, однако довольно часто это делают приглашенные специалисты, которые не осведомлены должным образом о новейших методах кибершпионажа, современных инструментах и направлениях киберпреступности.

В целях защиты от кибератак организации должны проводить постоянное инструктирование пользователей по вопросам компьютерной безопасности в отношении личных и корпоративных данных и объяснять правила публикации информации в социальных сетях. Применение программных средств защиты не может гарантировать полную защиту информации, поэтому крайне важно, чтобы соблюдение сотрудниками мер информационной безопасности стало частью стратегии защиты компании.

В список лиц, которым необходимо специальное обучение по информационной безопасности, следует включать:

– сотрудников, занимающих ключевые посты в разработке информационной системы;

– сотрудников, занимающих ключевые посты в эксплуатации информационной системы;

– должностных лиц организации, руководящих разработкой проекта информационной системы и программы обеспечения ее безопасности;

– сотрудников, несущих административную ответственность за безопасность, например контролирующих доступ или управляющих директориями [2].

Помимо данных категорий сотрудников, следует проводить обучение тех лиц, которые направляются в командировки, будут заняты работой в дистанционном режиме, а также в отношении которых собраны данные о наличии инцидентов в области информационной безопасности.

Исходя из приведённой информации, предлагаются следующие базовые сценарии обучения в зависимости от возможных рабочих обстоятельств (рисунок 1).

Рисунок 1 – Возможные сценарии обучения

1. курс «Основы информационной безопасности» для новых сотрудников;
2. курс «Защита конфиденциальной информации»:

– для сотрудников, поступивших на новую должность;

– для сотрудников, в отношении которых собрана информация о прецедентах путем анализа журналов безопасности:

1. средств антивирусной защиты;
2. систем защиты информации (СЗИ);
3. DLP-систем;
4. Active Directory.

3. курс «Противостояние фишинговым атакам» для сотрудников, в отношении которых обнаружены соответствующие прецеденты;
4. курс «Информационная безопасность в условиях удаленной работы», для сотрудников, направляемых в командировки или занятых работой в дистанционном режиме.

В таблице 1 приведен список тем, предлагаемых для изучения на курсах.
Таблица1 – Категоризация тем курсов обучения информационной безопасности

Курс	Темы	Категории обучающихся
Основы информационной безопасности	- предупреждение нарушений конфиденциальности, целостности и доступности; - потенциальные угрозы, которые могут оказать неблагоприятное воздействие на производственную деятельность организации и сотрудников; - классификация чувствительности информации; - процесс обеспечения общей безопасности; - описание процесса обеспечения общей безопасности; - компоненты анализа риска; - меры защиты и обучение приемам их применения; - роли и обязанности сотрудников; - политика информационной безопасности.	Новые сотрудники

Продолжение таблицы 1

Защита конфиденциальной информации	- доступ к информации; - информационные системы; - обработка информации; - организация защиты информации; - административные меры защиты информации; - законодательные меры защиты информации; - программно-технические средства защиты информации; - криптографические методы защиты информации; - аутентификация субъектов доступа; - разграничение субъектов доступа; - протоколирование и аудит.	Сотрудники, поступившие на новую должность
Противостояние фишинговым атакам	- методы несанкционированного получения пароля; - особенности фишинга; - роль социальной инженерии в фишинг-атаке; - анализ используемых для атак инструментов; - комбинированные атаки с использованием фишинга; - методы и средства защиты личных данных; - методы и средства защиты корпоративной информации; - реакция на инциденты; - алгоритмы реагирования на инциденты.	Сотрудники, в отношении которых обнаружены инциденты
Информационная безопасность в условиях удаленной работы	- защита личных данных; - защита корпоративных данных; - реакция на инциденты; - основные приемы выявления уязвимостей; - безопасная работа в сети; - признаки атак; - методы обнаружения атак; - механизмы реагирования; - безопасное применение мобильных устройств.	Сотрудники, перешедшие на дистанционный режим работы

На рисунке 2 приведена схема предлагаемого алгоритма обучения сотрудников.

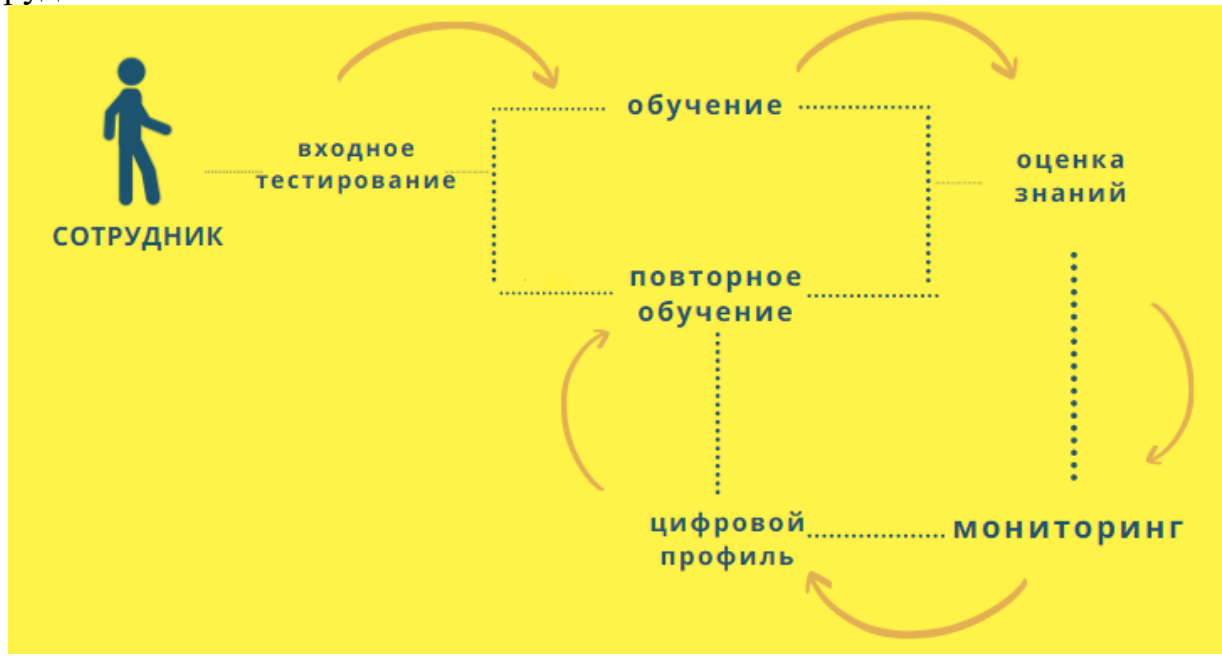

Рисунок 2 - Предлагаемый алгоритм обучения

Обучение может выполняться следующим образом:

1. входное тестирование для оценки исходного уровня знаний обучающегося. Входное тестирование необходимо для формирования понимания общего уровня осведомленности пользователей относительно цифровой грамотности;
2. обучение в рамках соответствующего курса;
3. оценка знаний по итогам пройденного обучения;
4. мониторинг деятельности сотрудника в аспектах, связанных с информационной безопасностью: анализ СЗИ, антивирусов, DLP-систем, анализ действий обучающегося при умышленном создании прецедента.
5. повторное обучение при необходимости.

Данной методикой предлагается формировать цифровой профиль пользователя, который будет создаваться в процессе профессиональной деятельности сотрудника. Цифровой профиль будет основываться на анализе работы специалиста, включая данные об успешности прохождения курсов, наличии инцидентов в области информационной безопасности. Информация о наличии инцидентов может быть получена путем анализа журналов безопасности средств защиты, а также исходя из сведений о действиях пользователя во время проведения имитационной атаки методом социальной инженерии. Такие учебные атаки предполагают умышленное создание ситуаций, в которых неграмотные действия пользователя могут привести к нарушению безопасности информации. Проведение тестовых нападений, помимо тренинга всего персонала, сможет выявить несовершенства используемых систем информационной защиты, проверить грамотность действий сотрудников безопасности.

Для проведения тестовых атак существует довольно много инструментов, доступных для реализации специалистами, например инструменты,

содержащиеся в дистрибутиве Kali Linux, однако разработки инструментария и сценариев атак должны быть индивидуальны для различных сетей и предприятий с учетом массы специфических параметров.

Проведение контролируемых атак – это единственный действенный способ снизить риски, связанные с хищением информации и денежных средств при использовании вредоносного программного обеспечения и неправомерного доступа к компьютерной информации.

Использование методов обучения в форме учений, приближенных к реальности, имеет сразу несколько положительных сторон. В результате проведенных тестовых атак специалисты могут разработать планы модернизации систем защиты и регламентов, а руководство может поощрить наиболее внимательных и бдительных сотрудников. Важным моментом при проведении тестовых атак и обучений является участие в них руководителей всех уровней, чего на практике часто не происходит. Все мероприятия проводятся лишь среди сотрудников [3].

Безопасное применение информационных технологий – важнейший шаг в формировании цифровой грамотности сотрудников многих предприятий. Особенно важным является обучение пользователей в тех организациях, где обрабатывается конфиденциальная информация. Ценность сотрудников, осознающих значимость защиты корпоративных данных, крайне выросла в связи с переходом на удаленный режим работы. Поэтому реализация, предложенного подхода к обучению сотрудников, важна с точки зрения фактического исполнения основных положений управления персоналом, закрепленных в политике безопасности предприятий.

Список литературы:

1. Tadviser: сайт /Информационная безопасность в компании — URL: https://www.tadviser.ru/index.php/Статья:Информационная_безопасность_в_компании (дата обращения: 05.03.2021). — Текст : электронный.

2. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

3. Масалков А. С. Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.: ил. ISBN 978-5-97060-631-5.