УДК 657.6

АУДИТ КИБЕРБЕЗОПАСНОСТИ

Клейменова Е. А.

Студентка 4 курса Факультета трансферных специальностей.

Ульяновский государственный университет,

Ульяновск, Россия

Сосунова Л. С.

к.э.н.,доцент,

Ульяновский государственный университет,

Ульяновск, Россия

Аннотация: Данная статья посвящена вопросам кибербезопасности, а именно: почему необходимо формировать культуру безопасноти на своем предприятии; как правильно провести аудит кибербезопасности и на что следует обратить внимание при проведении данной проверки.

Ключевые слова: кибербезопасность, защита информации, аудит, угрозы.

CYBERSECURITY AUDIT

Kleimenova E. A.

4th year student of the Faculty of transfer specialties.

Ulyanovsk state University,

Ulyanovsk, Russia

Sosunova L.S.

Ph. D.,associate Professor,

Ulyanovsk state University,

Ulyanovsk, Russia

Abstract: This article is devoted to cyber security issues, namely: why it is necessary to form a security culture in your enterprise; how to conduct an audit of cybersecurity and what you should pay attention to when conducting this audit.

Key words: cybersecurity, information protection, auditing, threats.

Тематика угроз кибербезопасности в данный момент крайне актуальна. Буквально каждый день в СМИ бывают замечены анонсы о взломе хакерами очередной системы и утечке конфиденциальной информации. Это связано с непрерывной цифровизацией бизнеса и государственных учреждений, а также увеличением количества угроз со стороны киберпреступников. Угроза подстерегает пользователей на каждом шагу. В настоящий момент для заражения компьютера вирусом достаточно кликнуть, к примеру, по баннеру на официальном веб-сайте широкоизвестного СМИ – вы автоматически перейдете на зараженный сайт, и на ваш компьютер будет скачан так именуемый «exploit kit», который сразу же начнет анализировать установленное у вас программное обеспечение на наличие уязвимостей [1].

Вопросы кибербезопасности стали чаще дискуссироваться в компаниях на всех уровнях управления. В свою очередь Служба внутреннего аудита при формировании годового плана должна основываться на оценку рисков, при этом нужно принимать во внимание мнение менеджмента и совета директоров.

При оценке рисков в области кибербезопасности необходимо рассмотреть следующие вопросы:

- Как тесно бизнес компании связан с информационными технологиями (далее ИТ)? Если это банк, то каждое нападение и несоблюдение работы ИТ-сервисов будет напрямую воздействовать на удовлетворенность клиентов и репутацию банка. В случае это сельскохозяйственная компания, то взлом сервера не будет сильно воздействовать на процессы внесения удобрений или же сбора урожая.

- Какие информационные системы (далее – ИС) и ресурсы используются? Насколько они критичны? Для этого необходимо понимать,

какой вред будет нанесен компании, если нарушатся такие характеристики информационных ресурсов как конфиденциальность, доступность и целостность. К примеру, несоблюдение конфиденциальности приведет к утечке секретной информации (информации о клиентах, индивидуальные данные служащих, итоги изучений и разработок) в открытый доступ или к конкурентам, что в свою очередь с большой вероятностью может привести к оттоку клиентов, либо к потере конкурентного преимущества. Несоблюдение доступности ИС может в большинстве случаях приводить к приостановке бизнес-процесса. Нужно определить реальную зависимость от данной ИС, т.к. довольно нередко главные бизнес-процессы компании (такие как обслуживание клиентов или отгрузка продукции) могут работать какое-то время и без средств автоматизации. Это конечно может привести к временным сложностям, но зато не даст возможности киберпреступникам заблокировать работу компании. Информацию с бумажных носителей в ИС можно внести позднее, после восстановления ее работоспособности. Несоблюдение целостности можно рассмотреть на примере несанкционированного внесения изменений в информацию – корректировка реквизитов контрагента с целью получения платежей, предназначенных для данного контрагента. При этом система внутреннего контроля в области платежей в компаниях как правило развита довольно хорошо.

Если в подразделении имеется сотрудник с опытом работы в ИТ или аудитов ИТ, этого может быть достаточно для проведения аудита кибербезопасности. По причине того, что область кибербезопасности постоянно развивается, данного сотрудника необходимо будет направить на получение дополнительного образования, где он изучит актуальные современные угрозы, векторы атак, а также способы защиты от них [2].

Если в службе внутреннего аудита нет специалистов в области ИТ, необходимо рассмотреть вопрос о привлечении внешних экспертов.

После распределения ресурсов, начинается планирование и предварительное обследование. На данных этапах необходимо определить, какие ИС и/или юридические лица и/или физические площадки будут рассматриваться.

После предварительного обследования наступает этап детального тестирования. По причине того, что любые настройки в ИС можно легко изменить, а выгрузки скорректировать, то при тестировании рекомендуется, предварительно получив необходимые полномочия для проверки ИС, не запрашивать данные удаленно, а исследовать ИС самостоятельно.

Особое внимание нужно уделить вопросам реальной безопасности, к примеру:

- Проводится ли тест на проникновение? Кто проводит? Цель исполнителя? Границы данного проекта? Каковы результаты? Исправляются ли выявленные недостатки?

- Как показывает практика, наиболее слабым звеном в системе безопасности считаются пользователи. В следствие этого нужно понять, как обучают пользователей задачам кибербезопасности? Оценивается ли их степень знаний?

- Какие инциденты ИБ были зафиксированы за аудируемый период? Как реагировали ИБ-специалисты? Велось ли расследование? Какие меры предпринимались по предотвращению данных инцидентов в будущем?

По результатам аудита рекомендуется сделать два отчета. Один отчет должен содержать детальное описание недостатков с использованием специфических ИТ терминов и быть направлен ИТ-специалисту. Второй отчет или презентация должен содержать описание ключевых моментов на так именуемом «языке бизнеса» для топ-менеджмента и аудиторского комитета [3].

Если раньше аудит кибербезопасности считался узкоспециализированным, специфическим и своеобразным, то в настоящее время данные проекты ведутся все чаще, а их итоги могут помочь фирмам улучшить безопасность бизнеса, спасти его от киберугроз и понизить затраты в представленной области.

Библиографический список:

1. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 1. / А.А. Карцхия // Вопросы кибербезопасности. - 2014. - №5. - С. 58-62.
2. Булай Ю.Г., Булай Р.И. Профилактика и противодействие киберпреступности, а также международным киберугрозам. / Ю.Г. Булай, Р.И. Булай // Академическая мысль. - 2017. - №8. - С. 110-118.
3. Массель Л.В. Кибербезопасность как одна из стратегических угроз энергетической безопасности России. / Л.В. Массель // Вопросы кибербезопасности. - 2016. - №12. - С.27-32.

Оригинальность 90%