b_152

Как «выбить» бюджет на ИБ у ректора:

Три важных слайда, которые работают

Спикер

Егор Андюков

Ведущий специалист по информационной безопасности

b_152

b_152

Более 14 лет профессионально обеспечиваем компаниям соответствие законодательству Российской федерации в области защиты персональных данных и информационной безопасности.

TATNEFT

самолет

ПЕРВАЯ БАШЕННАЯ TOWER.ONE

ТЕХНОНИКОЛЬ

PORSCHE

Экспобанк

SCHNEIDER GROUP
EXPERIENCE. EXPERTISE. EXCELLENCE.

Т БАНК

CHERY

ЦЕЛЬ

Сформировать план действий ответственных по ИБ в ВУЗах для выделения бюджета на информационную безопасность.

ЧТО ВЫ ПОЛУЧИТЕ:

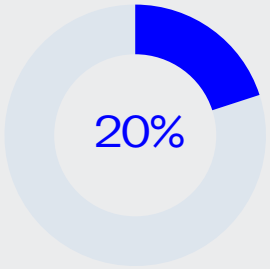
1. Подсветим статистику инцидентов ИБ в ВУЗах;
2. Разберем “красные флаги” проблем ИБ в ВУЗах;
3. Вспомним обязанности ВУЗа в обеспечении ИБ;
4. Сформируем формулировки с которыми можно идти к ректору.

ИНЦИДЕНТЫ В ВУЗах

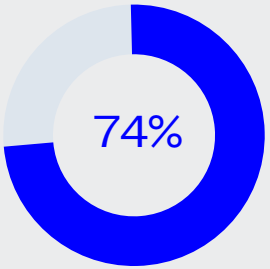
b_152

www.b-152.ru

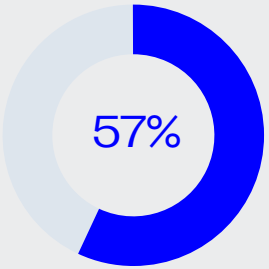
ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ В СФЕРЕ ОБРАЗОВАНИЯ В 2024 — 2025 г.



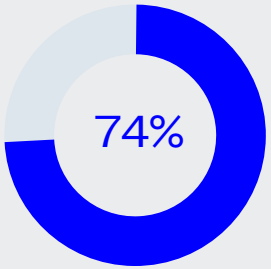
Утечки данных в образовании РФ



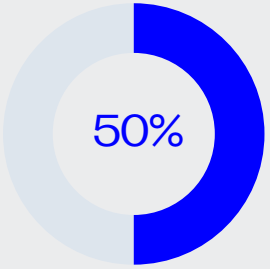
Инциденты ИБ в образовании



Атаки на ВУЗы



DDOS-атаки во время приемных кампаний



Бот-трафик на сайтах ВУЗов

ПРИЧИНЫ

Отсутствие выделенной функции
Ответственность возложена на проректора

Обучение ИБ
Устаревшие материалы или отсутствие обучения

Точечные меры безопасности
Меры реализуются без системного администрирования

Ограниченный контроль сервисов
Контроль внешних сервисов ограничен договорными отношениями

Техническое администрирование
администрирование выполняют студенты и непрофильные сотрудники

Отсутствие специалистов
Квалифицированные кадры уходят в коммерческий сектор

Устаревшие нормативные акты
Локальные нормативные акты и модели угроз устарели

Фрагментарные зоны ответственности
Ответственность распределена между различными подразделениями.

ОБЯЗАННОСТИ ПЕРЕД ЗАКОНОМ

Федеральный закон № 152-ФЗ «О персональных данных»

Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Постановление Правительства РФ № 1236 от 16.11.2015 «Об установлении запрета на допуск иностранного программного обеспечения»

Приказ ФСТЭК России № 31 от 14.03.2014 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры»

Указ Президента РФ № 250 от 01.05.2022 (ред. 13.06.2024) «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Приказ ФСБ России № 378 от 10.07.2014 «Об утверждении требований к средствам криптографической защиты информации»

Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных»

Приказ Минобрнауки России № 853 от 29.08.2013 «Об утверждении Положения об обеспечении защиты информации в информационных системах в сфере образования»

Постановление Правительства РФ № 1119 от 01.11.2012 «О мерах по обеспечению безопасности персональных данных при их обработке в информационных системах»

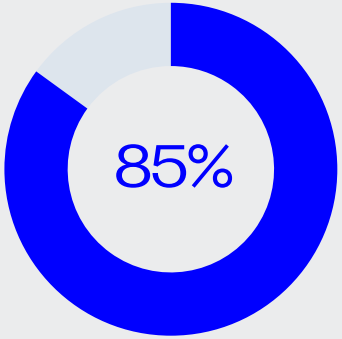
Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

ИССЛЕДОВАНИЕ ЗРЕЛОСТИ ИБ В РОССИЙСКИХ ВУЗах

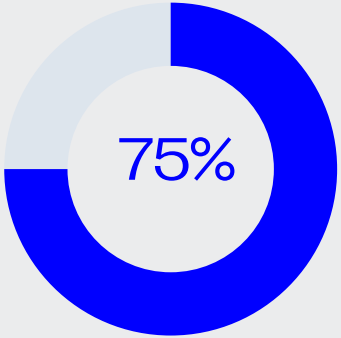
b_152

www.b-152.ru

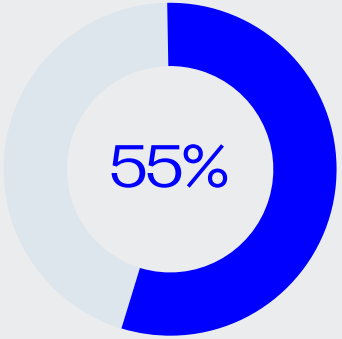
ИССЛЕДОВАНИЕ ЗРЕЛОСТИ ИБ В РОССИЙСКИХ ВУЗах



Резервное копирование и DR-планы



Антиспам и антифишинг-системы



Ежегодный самоаудит по ИБ и ПДн

ОСНОВНЫЕ ПРОБЛЕМНЫЕ ЗОНЫ

Управление уязвимостями:

65% — не проводится или выполняется нерегулярно.

Инструменты ИБ:

- SIEM — 25%,
- DLP — 25%,
- EDR — 10%,
- MFA — 10%,
- SOC/MSSP — 10%,
- MDM — 0%.

Документы по ПДн:

Средний показатель — 2 из 4 обязательных элементов в наличии.

- ОРД — 60%,
- Реестр — 55%,
- Договоры — 30%,
- Трансграничка — 15%;
- “Не знаю” — 30%).

Журналирование событий:

Длительное хранение логов (≥12 мес) обеспечено лишь у 40%.

Контроль облачных сервисов (LMS, прокторинг, биометрия):

- 85% ограничиваются договорами,
- оценку рисков проводят лишь 15%,
- DPIA-подобные процедуры — 5%.

Организационная зрелость:

Медиана Индекса зрелости процессов (ИЗП) — 32,3 из 100.

Отсутствует формализованный инцидент-менеджмент, обучение персонала и планирование.

Фиксирование инцидентов

45% — не фиксировали инциденты;

30% — не могут оценить;

25% — сообщают о фактах нарушений.

Обнаружение инцидентов

60% — обнаруживают инциденты случайно,

25% — через мониторинг или SIEM/SOC.

MTTD/ MTTR:

В среднем 1–3 дня;

Оперативное реагирование («часы») — 10%.

Ресурсный голод — главная болевая точка

У большинства — <10 человеко-часов в неделю на всю ИБ-повестку.

Нехватка компетенций

Кадровый состав подразделения ИБ как правило состоит из бывших студентов, не имеющих реальной практики работы у интеграторов или в консалтинге. Опыт либо передает предшественник, либо вырабатывается самостоятельно.

Отсутствие CISO с глубоким знанием ИБ и опытом.

Как правило, за ИБ в ВУЗе отвечает проректор, который назначен номинально на должность, не имеет представления о том, как должна выстраиваться система защиты информации, тем более не понимает пул мер, которые необходимо реализовывать во исполнение требований по защите информации.

Процессы защиты информации не выстроены

Не введен системный подход PDCI в процесс построения системы защиты информации как на организационном уровне, так и на техническом.

В основном меры носят стихийный характер, по принципу “нас заставили это внедрить”.

Готовность к проверке — «средняя по больнице»

Документы и самоаудит частично есть, но «тонкие» элементы проектирование СЗИ, наличие актуальных конфигураций СЗИ, настройка встроенных механизмов защиты, сканирование уязвимостей, реагирование на инциденты , договоры с обработчиками, cloud-риски) часто провисают.

Обнаружение инцидентов чаще случайно

Следствие отсутствия мониторинга и практик.

Поддержка ректората реально двигает процесс

Там, где есть приоритизация и KPI, индексы готовности выше.

Большие ВУЗы более зрелые

Очевидно — за счет масштаба, ИТ-штата и внимания к комплаенсу.

ИБ = Снижение ожидаемого ущерба + Соблюдение закона + Сохранение имиджа

РИСКИ И НЕСООТВЕТСТВИЯ

Риск	Ущерб	Негативные последствия для бизнеса
Использование несертифицированного средства межсетевого экранирования	– Возможность утечки. – Штраф на юридическое лицо – в связи с увеличением оборотных штрафов до 3 000 000 – 15 000 000 р.	– **Технические риски:** нарушение защищенности систем (преднамеренное или случайное) ввиду ограниченных возможностей сканеров – **Юридические риски:** проверки регуляторов – **Финансовые потери и штрафы:** Штрафы, (оборотные, компенсации субъектам ПДн)
Возможность несанкционированного доступа и утечки информации при работе сотрудников с личных ПК, ноутбуков	– Несанкционированный доступ к защищаемой информации; – Кража коммерческой тайны; – Возможность утечки, – Штраф на юридическое лицо – в связи с увеличением оборотных штрафов до3 000 000 – 15 000 000 р..	– **Технические риски:** нарушение защищенности систем (преднамеренное или случайное) ввиду использования личных ПК, ноутбуков, утечка информации ввиду копирования на личные средства персональных данных и другой чувствительной информации. – **Финансовые потери и штрафы** (оборотные, компенсации субъектам ПДн
Отсутствует матрица контроля прав доступа пользователей в системе идентификации и аутентификации	– Возможность утечки – Штраф на юридическое лицо – в связи с увеличением оборотных штрафов до 3 000 000 – 15 000 000 р.	– **Технические риски:** БД оказалась в открытом доступе, в том числе в даркнете, простой в работе ИСПДн, необходимость дополнительных затрат на восстановление деятельности. – **Юридические риски:** проверки регуляторов

b_152

ЧЕК-ЛИСТ САМОКОНТРОЛЯ ПО ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ

ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ:
ЦЕНА РИСКА VS. ЦЕНА ЗАЩИТЫ

Варианты закупки (выбрать 1)	Артикул	Название позиций	Цена (указана примерно)	Кол-во	Стоимость (указана примерно)	Состав закупки (уточнение)	Места установки	Ссылка на продукт/Аналитику	Обоснование необходимости закупки	КП от вендора (получено/ не получено)
КОМПЛЕКС КОНТРОЛЯ И АНАЛИЗА ЗАЩИЩЕННОСТИ										
1вариант	PT-XS-IP16	Программное обеспечение XSpider. Лицензия на 16 хоста, обновления в течение 1 (одного) года	59150	1	59150	Лицензия срочная - 1 год	АРМ администратора ИБ (запуск ппо требованию, но не реже 1 раза в неделю)	https://www.ptsecurity.com/ru-ru/products/xspider/	1. Нейтрализация актуальных УБИ (обнаружение уязвимостей в ОС,ПО, прошивках коммутационного оборудования) 2. Реализация подсистемы контроля и анализа защищенности (группа мер АНЗ) 3. Реализация подсистемы	
	PT-XS-IP16-ADD	Программное обеспечение XSpider. Лицензия на дополнительный хост к лицензии на 16 хостов	2873	4	11492					
2 вариант	SCANER-VS-7-16-F	Средство анализа защищенности «Сканер-ВС». НПЕШ.00606-01. Лицензия на 16 IP адресов на 1 год (рег. № 231)	54000	1	54000	Лицензия срочная - 1 год	АРМ администратора ИБ (запуск ппо требованию, но не реже 1 раза в неделю)	https://scaner-vs.ru/		
	SCANER-VS-7-50-ADD-B-F	НПО «Эшелон» СКАНЕР-ВС (дополнительный IP к лицензии на 1 год)	3000	4	12000					
3 вариант	RC-C-Pro-License-1Y	Лицензия на использование программы Средство анализа защищенности RedCheck для оказания услуг сторонним организациям, редакция Professional на 1 IP-адрес на 1 год	2500	20	50000	Лицензия срочная - 1 год	АРМ администратора ИБ (запуск ппо требованию, но не реже 1 раза в неделю)	https://www.redcheck.ru/ Обзор сканеров: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets#part5		
	RC-Media kit	RedCheck. Медиа-комплект	1430	1	1430					

b_152

РЕЕСТР СРЕДСТВ ЗАЩИТЫ ОТ ИБ-КОМАНДЫ Б-152

СОСТАВЛЕНИЕ ПЛАНА И KPI ДЛЯ ОЦЕНКИ НА БЛИЖАЙШИЙ КВАРТАЛ — 12 недель

Недели 1–2 — организационный запуск

Недели 3–6 — базовая защита и учет

Недели 7–10 — мониторинг и восстановление

Недели 11–12 — обучение и регламентирование

СОСТАВЛЕНИЕ ПЛАНА И KPI ДЛЯ ОЦЕНКИ НА БЛИЖАЙШИЙ КВАРТАЛ — 12 недель

Недели 1–2 — Организационный запуск

- ☐ Приказ о назначении зам. руководителя по ИБ (если его не было).
- ☐ Формирование рабочей группы (ИТ, юристы, учебная часть).
- ☐ Инвентаризация информационных систем и ПДн.
- ☐ Составление реестра и проверка договоров.

СОСТАВЛЕНИЕ ПЛАНА И KPI ДЛЯ ОЦЕНКИ НА БЛИЖАЙШИЙ КВАРТАЛ — 12 недель

Недели 3–6 — базовая защита и учет

- ☐ Настройка журналирования ≥ 12 мес.
- ☐ Внедрение MFA в критичных системах.
- ☐ Периодические сканирования уязвимостей и обновления ПО.
- ☐ Пилот EDR на серверы и критичные АРМ.

СОСТАВЛЕНИЕ ПЛАНА И KPI ДЛЯ ОЦЕНКИ НА БЛИЖАЙШИЙ КВАРТАЛ — 12 недель

Недели 7–10 — мониторинг и восстановление

- ☐ Подключение SIEM-лайт или MSSP/SOC-as-a-Service.
- ☐ Проведение теста восстановления из бэкапов (с фиксацией времени и отчетом).

СОСТАВЛЕНИЕ ПЛАНА И KPI ДЛЯ ОЦЕНКИ НА БЛИЖАЙШИЙ КВАРТАЛ — 12 недель

Недели 11–12 — обучение и регламентирование

- ☐ Обучение ИБ-команды (комплаенс и реагирование).
- ☐ Обучение пользователей (фишинг, пароли, инциденты).
- ☐ Утверждение Плана реагирования (роли, эскалация, окна работ).
- ☐ Подготовка квартального отчёта для ректората.

Ваши вопросы?

b_152

САЙТ
b-152.ru

TELEGRAM
@ b152privacy

TELEGRAM
Чат экспертов

info@b-152.ru
+7 (499) 372-06-52